Maritime Security Requirements for Shipping Companies and Ports: Implementation, Importance and Effectiveness

Elena Sadovaya1*, Vinh V. Thai2

1 Division of Infrastructure Systems & Maritime Studies, School of Civil and Environmental Engineering, Nanyang Technological University, Singapore, N1-B4b-07, 50 Nanyang Avenue, Singapore 639798
Tel: +65 97720702, Email: elena2@e.ntu.edu.sg

2 Division of Infrastructure Systems & Maritime Studies, School of Civil and Environmental Engineering, Nanyang Technological University, Singapore, N1-01c-81, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 5331, Email: vvrthai@ntu.edu.sg

* corresponding author

Abstract

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 has come into force and imposed a long list of compulsory and voluntary maritime security requirements on shipping companies and ports. Existing data show that not all of these requirements are generally implemented. One of the reasons is the lack of resources needed for the implementation of those requirements, another is the misunderstanding of their importance. Besides, some of the implemented requirements may be found ineffective in achieving their intended goals. Therefore, the main objectives of this study are to identify the security requirements imposed on shipping companies and ports, to investigate which of them are generally implemented, and to explore the perceived importance and observed effectiveness of these requirements. To achieve the expected objectives, a comprehensive literature review of maritime security regulations and relevant literature was done to compose a detailed list of requirements for shipping companies and ports, and in-depth structured interviews with industry professionals have been conducted to obtain the information about the existing situation in their organizations. The findings of the study showed that majority of listed requirements were implemented in interviewed organizations. Several of the compulsory requirements were found not important or not effective for security improvement, however they were implemented because of their mandatory nature. Meanwhile, some of the voluntary requirements were not implemented, if they were found unimportant or ineffective by the organizations. Moreover, the different interviewees’ opinions about the importance and effectiveness of some security requirements can lead to a conclusion about different approaches chosen for security management in the organizations. Additionally, as collateral results, this paper provides some proved impacts of implementation of security requirements on the organizational performance of shipping companies. These findings have both academic and managerial implications. They can be useful for researchers working on the related topics, for security managers in shipping companies and ports, as well as for regulatory bodies when considering changes in maritime security related documents.

Keywords: Maritime Security, Security Regulations, Security Requirements

1. Introduction

1.1. Background Information

The problem of maritime security has existed for hundreds of years. Piracy, cargo pilferage, smuggling, stowaway were considered as prime issues. For a long time, there were no legal ways to deal with these problems. Different international and national organizations have tried to improve the situation by introducing various rules and conventions, such as the International Convention for the Safety of Life at Sea (SOLAS) and Convention for the Suppression of Unlawful Acts against the
Safety of Maritime Navigation (SUA Convention) (IMO, 1974, 1988). The 9/11 event in 2001 and the bombing of the French oil tanker Limburg in October 2002 made maritime security a hot issue in the international maritime agenda with a strong orientation on anti-terrorism actions. During a short period of time after these events a lot of new maritime security regulations and best-practice documents came into force. Nowadays there are significant number of conventions, codes, standards, programs, and other documents regulating maritime security, which impose a long list of compulsory and voluntary security requirements on shipping companies and ports.

1.2. Problem Identification

The diversity of maritime security initiatives poses a very important problem for shipping companies and port operators - how to meet and maintain all existing requirements in maritime security area, while not jeopardizing organizational performance. The implementation of these regulations is a very costly and time-consuming process and requires a lot of other resources. However, benefits from the implementation of a new security regime are still not clearly identified, whereas some shipping companies and ports even have reported negative impact on their organizational performance (APEC, 2002; Banomyong, 2005; Eyefortransport, 2002; Thibault et al., 2006; Timlen, 2007; Voort et al., 2002). Therefore, some doubts may appear in the maritime industry regarding the necessity to implement all proposed security requirements. Just a few papers have been conducted on studying the implementation of maritime security measures (Gutiérrez et al., 2007; Thai, 2007; Voss et al., 2009). Moreover, there is not much information regarding their importance and effectiveness. The question whether the perceived importance of security requirements may affect their implementation or not has not been studied a lot. Thus, to fill the existing gap and in this way to increase the understanding of the current security regime in the shipping industry, it is necessary to study the implementation of maritime security requirements, their importance and effectiveness.

2. Literature review

2.1. Maritime security regulations and requirements for shipping companies and ports

2.1.1. Regulations

As a part of maritime law, maritime security regulations have a very diverse nature. The maritime security requirements for shipping companies and ports may be found in various sources. In some literature these sources are divided into three sets (Bichou et al., 2007; Gutierrez & Hintsa, 2006; Talley, 2008).

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, as well as on port facilities serving such ships. The Code of Practice on Security in Ports provides detailed guidance for implementation of port security related requirements contained in the ISPS Code (IMO & ILO, 2003). The Seafarers’ Identity Documents Convention is another document from these 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 has been introduced at the national and regional levels. It includes states’ national regulation, as well as programs, rules or agreements developed by unions of countries. The set represents a mix of mandatory regulations and voluntary programs, each of those should be consistent with international legislation. The most significant documents of the second set have been introduced in the United States (US), the European Union (EU) and Asia-Pacific Economic
Cooperation (APEC) Region. After the terrorist attack in September 2011, US government started a very aggressive policy for protection of the national security. Since that time a lot of new security regulations have been developed and implemented in different areas of security, and, *inter alia*, in maritime security. One of the substantial US introductions is the Container Security Initiative (CSI) (CPB, 2002). CSI is a series of bilateral agreement between the US and foreign-trade country partners, aiming to identify high-risk US-bound containers in foreign ports before loading, using X-ray and gamma-ray technology. The Secure Freight Initiative (SFI) is a part of US layered approach to cargo security, and based on partnership with foreign governments, container terminal operators, and shipping companies about technologies of container scanning (DHS & DoE, 2006). 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 complementation to CSI, compulsory applicable to all US-bound cargo (DoT, 2002). Import Security Filling 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 US Customs and businesses involved into shipping of goods to 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 contracting relationship with US Customs and enjoy 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).

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 transports into EC law a mandatory part A of the ISPS code and Chapter XI-2, and make some paragraphs of Part B compulsory for Member States. It also widens 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 relating 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 Smart and Secure Tradelanes (SST) Initiative developed in 2002 by Strategic Council on Security Technology (SCST, 2002) in that the world’s three largest port operators – Hutchison Port Holdings (HPH), P&O Ports and Port of Singapore Authority (PSA) Corporation – cooperate to implement automated tracking detection and security technology for containers bounding for US ports. Moreover, the ISO’s “Specification for Security Management System for the Supply Chain” 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 into mandatory and voluntary nature. Mandatory regulations contain compulsory requirements in terms of implementation. These requirements may be compulsory for all members of shipping industry, regardless of area of their operation, or only for those, operating in a specific region or under specific conditions. Meanwhile, requirements of voluntary nature are not compulsory for implementation. However, as several authors believe, some of them may eventually become a minimum criteria for participating in international trade, as non-compliance often has a negative effect on business performance of shipping companies and ports (Altemöller, 2011; Banomyong, 2005; Gutierrez & Hintsa, 2006; Metaparti, 2010; Rice Jr & Spayd, 2005). Table 1 shows two groups of maritime security regulations: regulations imposing compulsory security requirements and those containing voluntary recommendations.

2.1.2. Requirements

The regulations as reviewed above impose a long list of various security requirements on shipping companies and ports. However, it is observed that some of the requirements often repeat each other. Nowadays, one of the most discussed problems in the related literature is overlapping and inconsistency between the requirements imposed by different regulatory bodies (Bryant, 2009; Hintsa et al., 2009; Sarathy, 2006; Thibault, et al., 2006; Yang, 2010). Gould et al. (2010) 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.” As an 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 (Regulation No 725/2004), the US (ANOA) and Singapore regulations (DHS, 2003; EU, 2004; MPA). Besides, the requirement to submit cargo related information 24 hours before cargoes are loaded in foreign port is contained in regulations of different countries such as EU 24HR, US AMR, China 24HR, Canada 24HR, Mexico 24HR (CBSA, 2004; China Custom, 2008; DoT, 2002; EU, 2011; MCA, 2008). It can be argued that the discussed repetition and overlapping of security requirements can be a necessity in many cases, since international regulations are required to be made applicable within a country through enabling national legislations as well as some national regulations are only applicable to goods bound to the specific country. However, this overlapping brings additional problems to shippers and carriers, working with different countries of destinations. For example, Yang (2010) found that survey respondents often met the problem related to the extension of the 24HR to Canada and China: “the lack of uniformity among security initiatives and security transmission systems hinders transmission operations”; additionally, the extension of the rule “has created additional document data-input and cargo inspection costs for exporters and transporters”.

Moreover, majority of voluntary requirements are simultaneously found in different sources, such as WCO SAFE Framework of Standards, AEO Program, C-TPAT, STAR Initiatives, BASC, STP, and ISO Standards among others. This similarity between security requirements may benefit for shipping companies and ports, because compliance with one of the programs sometimes may be considered as a half-way to participation in another similar program since some of the requirements have been already implemented. However, Gutierrez & Hintsa (2006) 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”. Even though 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, “…in their specific purposes, the instruments they use, as well as their means of implementation” (Altemöller, 2011). As argued by Gutierrez & Hintsa (2006), “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”.

4
<table>
<thead>
<tr>
<th>Maritime security regulations</th>
<th>Regulations, containing compulsory requirements and requirements compulsory under specific conditions</th>
<th>Regulations containing voluntary requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For shipping companies</td>
<td>For ports</td>
</tr>
<tr>
<td>International</td>
<td>ISPS Code, Seafarers’ Identity Documents (SID) Convention</td>
<td>ISPS Code</td>
</tr>
<tr>
<td>National and regional</td>
<td>AMR (*for all cargo bound to US), 10+2 Rule (*for all cargo bound to US), ANOA (*for all cargo bound to US), EU Regulation No 725/2004 on Enhancing Ship and Port Facility Security (*all EU Member States), EU 24HR (*for all goods that are arrived to EU countries, Norway, Switzerland), Canada 24HR (*for cargo bound to Canada), China 24HR (*for cargo bound to China), Mexico 24HR (*for cargo bound to Mexico)</td>
<td>CSI (*traffic of cargo to US, agreement with US govt), SF1 (*traffic of cargo to US, agreement with US govt), EU Regulation No 725/2004 on Enhancing Ship and Port Facility Security (*all EU Member States),</td>
</tr>
<tr>
<td>Industry</td>
<td></td>
<td>ISO Standards, BASC</td>
</tr>
</tbody>
</table>

Note: * indicates conditions, if applicable.

**Abbreviations:** AEO, Authorized Economic Operator; AMR, Advance Manifest Rule; ANOA, Advance Notification of Arrival; BASC, Business Anti-Smuggling Coalition; CSI, Container Security Initiatives; 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; SFI, Secure Freight Initiative; SST, Smart and Secure Tradelanes; STAR, Secure Trade in the APEC Region; STP, Singapore Customs Secure Trade Partnership; 24HR, 24 Hour Rule.
Thus, the question about the necessity of unification of the existing common standards and maritime regulations, partly by mutual recognition concept, is widely discussed in the literature (Aigner, 2010; Altemölle, 2011; Gould, et al., 2010; Ireland, 2011; Metaparti, 2010; Mikuriya, 2007; Pallis & Vaggelas, 2008; Stasinopoulos, 2003; Voort, et al., 2002). Widdowson and Holloway (2009) believe that “there is a strong demand for standardization, harmonization and mutual (cross-border) recognition.” The problem of overlapping of security regimes was also discussed in the paper of Grainger (2007), in that the author used the concept of “security spaghetti” to describe the existing situation. However, just a few studies have been conducted on the comparison of security requirements imposed by different regulations. For example, Gutiérrez & Hintsa (2006) in their research combined security measures found in different voluntary supply chain security programs. Similarly, our paper provides a list of compulsory and voluntary security requirements for shipping companies and ports, most often met in different regulations.

Based on the review of regulatory documents and other related literature, it is concluded that there are ten most often met categories of security requirements, 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. In this study, to simplify the understanding of the information, ten categories were combined into four: 1. security onboard the ship and/or in port facility, that includes physical security, access control and cargo security; 2. personnel related security combines personnel security and security training and awareness; 3. cooperation with authorities regarding security issues, solely represented by the category of Cooperation with authorities; and 4. security of overall company management, which includes information and documentation security, security of business partners, crisis management and incident recovery, and security assessment, response and improvement. Table 2 provides a list of compulsory and voluntary security requirements for shipping companies and ports organized into four categories.

2.2. Implementation, effectiveness and perceived importance of maritime security requirement

Table 2 provides a comprehensive list of compulsory and voluntary maritime security requirements for shipping companies and ports. However, it is possible that not all of them are practically implemented. One of the reasons is the lack of resources needed for the implementation of those requirements, another is the misunderstanding of their importance. Not many studies have been conducted to verify the implementation of maritime security requirements. Gutiérrez et al. (2007) investigated which security measures were commonly implemented by BASC member companies, as well as 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. Moreover, the question about implementation and effectiveness of some security measures was also touched in studies of Voss et al. (2009), Gutiérrez et al. (2007) and Thai (2007). While Gutiérrez et al. (2007) studied effectiveness only with respect to security improvement, Voss et al. (2009) and Thai (2007) also looked at it in regard to some other organizational performance. Besides, there are some studies on the effectiveness of different security regulations, such as US CSI and C-TPAT, conducted by government bodies. They include different studies of the US Government Accountability Office (2008a, 2008b). These studies are important for studying the effectiveness of the whole specific regulation or initiative. However, they did not investigate the effectiveness of any single security measure composing the regulation.

Moreover, some authors believed that effectiveness of security requirements may vary in different cases, and approach to security management chosen by shipping companies and ports 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 and ports, which is widely discussed in maritime related literature, however not touched in this study, because it is a wide topic that requires further research.
Table 2 Compulsory and voluntary maritime security requirements for shipping companies and ports

<table>
<thead>
<tr>
<th>Categories</th>
<th>Compulsory requirements</th>
<th>For shipping companies</th>
<th>For ports</th>
<th>Voluntary requirements for shipping companies and ports, most often met in various voluntary security programmes</th>
</tr>
</thead>
</table>
| Security onboard a ship and/or in port facility | - develop SSP;  
- install SSAS and AIS;  
- display SIN;  
- ensure routing checking of cargo (ISPS Code); | - develop PFSP;  
- ensure routing checking of cargo (ISPS Code);  
- use NII and RD equipment to identify high-risk containers bound to US;  
- use optical scanning technology to identify high-risk containers (SFI). | - 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; |
| Personnel related security | - appoint CSO, SSO;  
- carry out training and drills (ISPS Code);  
- ensure SID is held by every seafarer (SID Convention); | - appoint PFSO;  
- carry out training and drills (ISPS Code); | - 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; |
| Cooperation and authorities regarding security issues | - 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); | - keep records of activities;  
- assure necessary security level of port facility (ISPS Code);  
- share the information with US CBP;  
- work with deployed foreign officers in the ports (CSI); | - continuing mutual exchange of information with authorities;  
- procedures for reporting to relevant authorities of any incidents; |
| Security of overall company management | - undertake SSA (ISPS Code); | - undertake PFSA (ISPS Code); | - 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. |

Additionally, it is important to study the effectiveness of security requirements because the lack of knowledge on this topic and misunderstanding of their importance may lead to unwillingness of shipping companies and ports to implement these requirements (Altemöller, 2011; Thibault, et al., 2006; Voss, et al., 2009; Yang, 2010). Moreover, not many papers have focused on studying the importance of security measures as perceived by managers of shipping companies and ports. Some authors just occasionally mentioned the attitudes of the managers towards the importance of one or the other security requirement (Bichou & Gray, 2004; Thai, 2007, 2009; Urciuoli et al., 2010) without a thorough scientific evaluation. Additionally, the question of how the understanding of the importance of security requirements may affect their implementation in shipping companies and ports, has not been studied extensively in the contemporary literature. It is therefore important that this question be addressed further as it implies how security could be managed effectively and contributes to overall business performance of a port or a shipping company.

3. Research methodology

3.1. The research questions

The review of related literature shows that not many studies have been conducted on the question regarding the implementation of maritime security requirements in shipping companies and ports, their perceived importance and effectiveness, as well as the connection between these issues. To fill this existing gaps this research aims to examine three research questions.

RQ1. What compulsory and voluntary security requirements are implemented by shipping companies and ports?

RQ2. Which of the compulsory and voluntary security requirements are considered as important by shipping companies and ports’ managers?

RQ3. Which of the compulsory and voluntary security requirements are viewed as effective, in respect to security and other organizational performance, by shipping companies and ports’ managers?

3.2. Method of data collection

Due to the exploratory nature of the research issues, the qualitative method is utilized in this study. The structured interview was applied as the method for data collection. This approach was chosen to make the interview process easier and more convenient for respondents. However, deviations during interviews were necessary to collect some clarifying information.

3.3. Sampling design

Due to the time constraint, three in-depth interviews were conducted. The interviewees were chosen among managers of shipping companies who are in charge of risk and security management such as company security officer, managers of safety and security departments, designated persons ashore etc. Their contact details were derived from existing Nanyang Technological University’s databases. The interviewed companies can be considered as big and well-established, two of them operate tankers, and the third company operates containerships.

3.4. Design of research instruments

The interview questionnaire consists of two parts. The first part contains a series of close-ended and open-ended questions designed to elicit participants’ views regarding the implementation of compulsory and voluntary maritime security requirements, their importance and effectiveness. The list of requirements was given to respondents during the interview. The second part is designed to solicit the classifying information regarding the interviewee’s organization and designation.

4. Findings and discussion
4.1. Implementation of security requirements

It was observed that interviewed organizations have implemented majority of the listed compulsory and voluntary requirements, with exclusions of those not applicable for the specific type of organization. For example, it was indicated by interviewees who are tanker operators that the following requirements are not applicable for their organizations: routing checking of cargo, submission of cargo related information 24 hours before cargo loading, submission of vessel stow plan and container status message, as well as written procedure for sealing of cargo and procedures for inspection of full and empty containers. Some of them appeared to be a participant of various voluntary partnership programs. It was commented that some voluntary requirements, such as access control, procedures for hiring of employees, screening of current and prospected employees, and some others, were implemented even before the organization’s participation in the program. Therefore, the changes of security measures for the certification purposes were not very significant and did not require big investments. However, interviewees indicated that they had to manage some problems, connecting to the lack of common procedure when implementing different voluntary security programs. Although several programs have mutual recognitions with each other, majority of them require separate certification. This is illustrated in one of the interviewees’ comment 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.*

Other interviewees consented that for their organizations a problem was that the implementation of security measures often depended on trading area, and that could pose the issue of the lack of unification of regulations while overlapping requirements exist. The US region was found the most troublesome in terms of restrictions and requirements. A typical comment by one of the interviewees is as follows:

*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 interviewees agreed upon the need for a common regulatory framework for all regions and countries. However, the opinion was expressed that “because of the political issue and opinions it’s not possible to make [such] common framework.”

According to the interviewees, only few compulsory requirements were not implemented. For example, one of the organizations did not conduct routing checking of cargo, but left this duty to other participants of the supply chain. This was explained by the good faith relationship between the organization and its business partners, as well as by strict procedures for choosing and assessment of business partners. Moreover, it was found that some of the interviewed organizations did not use SID. It was commented by some interviewees that their organizations used their own identification documents instead because of the convenience issue. Additionally, several voluntary requirements were found not implemented. For example, the security management systems (SMS) in interviewed organizations have been limited by development and assessment of SSPs: “we don’t usually keep separate management system besides that implemented under SSP.” Some of the interviewees included documents of compliance with voluntary programs in the organization’s SMS. One of the interviewee also mentioned that they issued some additional documents, such as security circulars and broadcasts. However, none of the interviewed organizations implemented any common system for the management of security.
Apart from the requirements from the list, interviewees identified other security measures implemented in their organizations, such as using tracking systems, carrying armed guards on board, designing citadels and safe master points onboard a ship with secure control, navigation and communication systems, developing 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 the respondents indicated that their organizations followed the recommendations of IMO Best Management Practice (BMP4) and, if necessary, IMO Guidance on the use of privately contracted armed security personnel on board ships. Moreover, one of the interviewed organizations was conducting the research on development of independent tracking system, operating when the power on board the ship is cut off.

4.2. Perceived importance of security requirements

Interviewees were asked to indicate their attitude towards the importance of implementation of specific security requirement for the purpose of enhancing security inside the organization and in the supply chain. It was observed that some of the compulsory requirements were not considered as important for security improvement. Among them were requirements to display SIN, use SID, install AIS, and keep records of activities and CSR. It was commented that these requirements were more important for compliance issue, rather than for enhancing of security, and they were implemented only because they are compulsory for implementation. Similarly, exchange of information with authorities was considered as important in terms of commercial and political issue, rather than security. Additionally, one of the interviewees did not consider screening of employees for security purposes as an important requirement. He believed that the probability of seafarers’ involvement in terrorism activity was very low and commented as follow: “I haven’t seen so far any person being terminated because of security purposes.” All other requirements from the list were recognized as important by all interviewees. They pointed out the importance of SSA and security training and drills, as it was believed that these measures significantly increased vigilance and awareness.

4.3. Effectiveness of security requirements

For the issue of effectiveness, interviewees were asked to indicate whether they found a specific security requirement effective in respect to security and other organizational performance. Security and other organizational performance were studied separately, to find out what other observed impacts of the implementation of security requirements were, apart from security improvement. For security matter, it is worth mentioning that some of the interviewed organizations consider security only as anti-piracy and anti-terrorism measures. It could be explained by the type of organizations. For example, security incidents such as pilferage or smuggling are not frequently observed onboard tankers. Besides, the possibility of the piracy or terrorist attacks is so small that some organizations do not have any statistics. Because of these facts, some interviewees could not give clear answer for the question about security improvement. However, they provided their evaluation of security effectiveness based on the crisis and incident exercises, conducted in their organization, as well as on the general company security culture. Among measures which were not considered as effective for security improvement, interviewees identified the following requirements: to install SSAS, IAS, to display SIN, to keep records of activities and CSR, and to obtain ISSC. However, all respondents agreed that the mentioned requirements can be useful for other purposes, such as post incident investigation, customs clearance, and navigation. Other requirements from the list were considered as effective. However, respondents admitted that some of them did not enhance security inside the organization but could help to improve public security, and they were implemented mostly because of their mandatory nature.

For the matter of effectiveness with respect to other organizational performance, interviewees were asked to provide their opinion on positive and negative impacts of the implementation of security requirements. In general, respondents’ opinion about this question was neutral. They could not clearly evaluate if the specific requirement were effective or had negative effects. However, some observations have been done. As mentioned earlier, some of the compulsory requirements, such as
AIS, SIN, records of activities, were found effective for the purposes of navigation and post-incident investigation. Additionally, requirements such as clear identification of organizational roles and responsibilities, periodic self-assessment and training on crisis management, resulted in positive changes of organizational procedures and technologies. Interviewees perceived that periodic assessment, as well as training, drills and exercises helped their organizations to identify possible incident causes, whereas identification of responsibilities improved feedback and cooperation with employees. Additionally, one of the interviewees indicated that after analyzing causes of security incidents the organization usually introduced to their customers new technologies or procedures, for example, GPS tracking or high security seals. He commented: “Some customers are very serious about security, others are not so. We need to find a balance.” Besides, it was found that the implementation of procedures for controlling all documents, data and information, as well as procedures for reporting to relevant authorities of any incidents helped organizations to keep customer information confidential and consequently to improve customer satisfaction and company image.

Some of the requirements were found negatively effecting organizational performance. Interviewees indicated that the implementation of requirements of the ISPS Code resulted in extra work and fatigue of the crew, extra jobs for the shore-based staff, and problems for crew to go ashore. Besides, access control created a conflict between security and safety, when doors, closed for security purposes, contradicted safety regulations. Moreover, it was mentioned that SSAS initially brought some problems related to false activation, however after some time the number of false alerts decreased significantly. Finally, the implementation of compulsory requirements, as well as some voluntary ones such as the installation and maintenance of tracking equipment, design of citadels, and the implementation of other anti-piracy measures, requires money, time, information, and advance planning. However, interviewees considered these efforts as a necessity and commented that gradually they became an important part of the everyday organizational activities.

It is observed from the above that several of compulsory requirements were not considered as important and effective for security improvement and were implemented mostly because of their mandatory nature. Meanwhile, majority of voluntary requirements were implemented because the organizations found them important for security purposes. Another important observation is that similar organizations had very different opinions about the effectiveness or importance of the same requirements. This implies the various approaches to security management in different organizations. Some of the interviews believed that the results of security implementation would depend on the approach of implementation of requirements. One of them commented about SSP as follows:

This ISPS requirement is good, but depends on how you do it. If you do a lousy job, of course your plan is not so good, not robust in emergency...

Finally, it was observed that even if interviewed organizations initially had some difficulties when implementing security requirements, nowadays they can manage security in a more effective way. Implementation of security requirements have become a part of everyday activity of the organizations, where required security investments have been balanced by increased taxes and rates, employees and crew have become more habitual with their security duties and responsibilities, customers have become more concerned about the time for delivery of cargo before shipment. These examples support the opinion that effective security management may help shipping companies to achieve positive results, specifically, to reduce negative impacts of implementation of security requirements and achieve more benefits.

5. Academic and managerial implications

Firstly, it was observed that majority of compulsory requirements are implemented in the organizations, however not all of them are considered as important or effective for security improvement. Meanwhile, voluntary requirements are implemented only if they are found important or effective. This topic has been poorly studied and can be developed further in the future research. Moreover, these findings can be useful for regulatory bodies when considering changes in security
related documents. Secondly, the difference in the interviewees’ opinions about importance and effectiveness of some security requirements may be caused by the different approaches chosen for security management in the organizations. The above findings therefore re-affirm that further research should be conducted in the area of maritime security implementation and management. Additionally, this paper and other similar publications can help security managers to change their opinion about different requirements and, therefore, change security management approach in their organizations. Thirdly, as collateral results, this paper provides some proved impacts of implementation of security requirements on organizational performance of shipping companies, which can be used for future research on this topic. Finally, it provides a comprehensive list of compulsory and voluntary security requirements for shipping companies and ports, which is useful for both academic and managerial purposes.

6. Conclusion, limitations and future research directions

This study aims at investigating the implementation, importance and effectiveness of maritime security requirements in shipping organizations. For this purpose, the combination of different research methods was employed, utilizing the comprehensive literature review to derive a list of compulsory and voluntary security requirements for shipping companies and ports and validate them through several structured interviews with industry professionals. The findings show that majority of listed requirements were implemented in interviewed organizations. Several of the compulsory requirements were found not important or not effective for security improvement, however they were implemented because of their mandatory nature. Meanwhile, some of the voluntary requirements were not implemented if they were found unimportant or ineffective by the organizations. Moreover, some positive and negative impacts of the implementation of security requirements on organizational performance were identified. Several positive impacts were named, such as reduced number of security incidents, increased security awareness, changes in processes and technologies, improved feedback and cooperation with employees, improved customer satisfaction and company image. Negative impacts include extra work and fatigue of the crew, extra jobs, problems for crew to go ashore, conflict between safety and security, as well as extra money, time, information and need for advance planning. Finally, it was concluded that the results of the implementation of security requirements could depend on the approach to security management in organizations.

This study is significant in two ways. Firstly, it provides a comprehensive list of compulsory and voluntary maritime security requirement for shipping companies and ports, which has not been composed before. This list can be used for other research in the related area, as well as by industry professionals for security management and assessment purposes. Secondly, no studies have been conducted before on the investigation of implementation, importance and effectiveness of both compulsory and voluntary maritime security requirements. The research questions examined in this study are significant for future research on the effective management of maritime security in shipping and port organizations.

Nevertheless, some significant limitations exist. The reliability of obtained results is reduced mainly due to the small number of interviews conducted. Additionally, the obvious sample bias is that all three companies are big and well-established in the shipping industry. It means that obtained results cannot accurately reflect the view of the whole industry. However, the study’s findings are sufficient to make some preliminary conclusions about the research topic and to infer that further research is necessary in the area of implementation, importance and effectiveness of maritime security measures. Therefore, in the future, more interviews and/or survey should be conducted with other shipping companies of small and medium size, port operators, as well as with shipping councils and professional bodies to obtain more accurate data that reflect the view of the industry.
References


BASC (2002), BASC Standards.


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


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


Department of Treasure, U.S. (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.

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

EU (2007), Authorized Economic Operators Programme.


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


