Impacts of security improvements on service quality in maritime transport : an empirical study of Vietnam

Thai, Vinh Van

2007

Thai, V. V. (2007). Impacts of Security Improvements on Service Quality in Maritime Transport: An Empirical Study of Vietnam. Maritime Economics & Logistics, 9, 335–356.

https://hdl.handle.net/10356/98495

https://doi.org/10.1057/palgrave.mel.9100188

IMPACTS OF SECURITY IMPROVEMENTS ON SERVICE QUALITY IN MARITIME TRANSPORT: AN EMPIRICAL STUDY OF VIETNAM

Vinh V. THAI
Department of Maritime and Logistics Management
Australian Maritime College
P.O. Box 986, Launceston, Tasmania 7250, Australia
Tel.: +61 3 6335 4764 Fax: +61 3 6335 4720
Email: V.Thai@amc.edu.au

Abstract

In recent years, maritime security has become a major concern on the international maritime agenda. If security measures and initiatives are not carefully designed and effectively implemented, they can negatively impact the whole maritime transport chain. Security improvements resulting from maritime security requirements may also bring about some benefits to service quality and business performance for the organisations. However, there are limited studies conducted on these aspects. In this paper, we aim to address these gaps by devising a framework of projected impacts of security on service quality in maritime transport and conducting an empirical study to verify the projection. The study was conducted in Vietnam with a group of shipping, port and freight forwarding companies, using the triangulation of both mail survey and in-depth interview techniques. It was evident from this study that all projected relationships between security improvements and service quality are supported by both survey respondents and interview interviewees. The statistical analysis reveals that, among the 13 projected relationships, respondents indicate clear consensus of agreement on seven projections, in which security improvements can enhance service quality in terms of increased reliability of service performance, social responsibility awareness, increased efficiency in operations and management, as well as enhanced image in the market. For the other projections, the respondents' agreement is not clearly shown. This is also reflected in interviews, in which respondents emphasise the most notable benefits brought about by security improvements are in terms of increased reliability of service performance, increased awareness and better image, thus positively affecting customers' perception of the organisation's service quality. However, these positive impacts are only realised should service providers in maritime transport employ effective security management strategies.

Keywords: *Security, service quality, maritime transport*

INTRODUCTION

In recent years, maritime security has become a major concern on the international maritime agenda. Various security measures and initiatives have been devised and implemented at the international, national and organisational levels, such as IMO's International Ship and Port Facilities (ISPS) Code, the United States' Customs–Trade Partnership Against Terrorism (C–TPAT), Container Security Initiative (CSI) and others developed by the International Labour Organisation (ILO) and World Customs Organisation (WCO). While the need for security in maritime transport is pervasive and prominent, some academic and industrial

reports reveal that if such measures and initiatives are not carefully designed and effectively implemented, they can negatively impact the whole maritime transport chain. At the same time, it is argued that security improvements resulting from maritime security requirements may also bring about some benefits to service quality and business performance for the organisations. However, there are limited studies conducted on this aspect and most of these studies are industrial reports that lack academic rigour and do not focus on the issue of how security improvements may affect the quality of services provided by key maritime transport service providers, e.g. shipping companies, ports and freight forwarders/NVOCCs. Another major limitation of these studies is that the expected positive impacts resulting from security improvements were subjectively projected by the researchers and research organisations rather than being the result of findings from empirical surveys of views and perceptions of relevant practitioners in the field. In this paper, these gaps are addressed by devising a framework of projected impacts of security on service quality in maritime transport and conducting an empirical study to verify the projection. The paper is organized in four sections. First, a research framework is provided devising the projected impacts of security improvements on service quality. This is followed by a description on methodology to conduct the empirical study. Research findings from the study are provided next. Finally, concluding comments and future research directions are outlined.

RESEARCH FRAMEWORK

Security improvements have impact on several aspects of service quality in maritime transport. First, we see that applications of information technology (IT) and other technological solutions are especially encouraged in security initiatives promoted by governmental, regional and international organisations. For some initiatives, the presence of IT technology plays the critical role for success. For others, radical changes in operating

practices are needed to comply with security requirements. Investments in IT and technology for security requirements serve two main security purposes: better control of visibility of the shipment under maritime transport, either in transit or at ports, and better management of information regarding the shipment. The CSI initiative, for instance, requests that US bound containers of higher security risk be inspected in key foreign ports before being loaded onboard ships. The 24-hour Rule, a critical part of this initiative, supports this inspection activity by requiring the shipment manifest to be submitted to US Customs 24 hours before containers are loaded on board. Such security requirements will hardly be complied with if the early reporting of cargo and schedule details is not facilitated by improved IT systems by shippers and shipping lines, freight forwarders or NVOCCs. The Smart and Secure Tradelane (SST) initiative, for example, aims at enhancing the control of shipment visibility while containers are on board the ships and at ports. The ISPS Code, which is applied to all signatory countries of the SOLAS convention, also requires ships and port facilities to install new equipment to improve their security, including the enhanced interchange of security information between ships and ports.

IT and technological solutions supporting security improvements will potentially benefit not only security but also some quality factors. With investments in technological solutions such as electronic seals and RFID and supporting IT infrastructure, the control of shipment visibility during transit and at ports can be facilitated and therefore the shipment tracing capability of shipping lines, port operators and freight forwarders/NVOCCs can also be enhanced. Aichlmayr (2003) argued that about 6–10% of money spent on transporting goods is wasted as a result of inaccurate, inadequate or insufficient information. If shipment data can be captured in real time, companies can make supply chain adjustments in real time. Investment in IT and EDI is unavoidable if organisations, both shippers and maritime

transport service providers, are to comply with security requirements, such as early reporting and exchange of cargo and schedule details. With IT and EDI systems in place, many benefits result such as lower payroll due to improvements in IT infrastructure (OECD, 2003). Hence, security improvements resulting from IT, EDI and technology investments may have a positive impact on service quality of maritime transport when shipment tracing capability is enhanced.

It is argued that the speed of maritime transport service provided by shipping lines, port operators and freight forwarders/NVOCCs may be potentially facilitated by the application of IT and EDI systems and the related changes to current operating practices. Integrated IT and EDI systems among service providers and their customers would allow them to better manage shipment information, thus resulting in faster processing time (OECD, 2003), and subsequent higher service performance. With the early submission of shipment information, shipping lines, port operators and freight forwarders/NVOCCs will have better control in their planning and management, thus facilitating the performance of their service delivery. For port operators, specifically, this practice would be very useful in early targeting of shipments for inspection, and therefore avoiding congestion in handling of other shipments. Investment by Customs in IT and EDI systems for security enhancement would also indirectly support the maritime transport service providers enhancing the speed of their services. Moreover, in transport, the reliability of service is critically important, since logistics costs increase and service levels decline as reliability of service—for example delivery time reliability—decreases. Quality increases as variability decreases. The main purpose of security control and management is to drive out the variability of pick-up, transit and delivery time, therefore increasing the reliability of service (Wolfe, 2002). Security improvements can also help maritime transport service providers in having better shipment

loss and damage control; in other words, shipment safety and security. The impact between security improvements and shipment safety and security is the most direct and comprehensible. The importance of security improvements in this respect has long been acknowledged as a contributing factor to increase profits for organisations. Sennewald (1978) argues that security contributes to company or corporate profit by reducing or eliminating preventable losses. In maritime transport, in addition, cargo loss and damage records have always been considered an indicator of service quality.

Security improvements also impact on the reliability of documentation, so that documentation processes conducted by maritime transport service providers can be potentially free from errors. It has been argued that the accuracy and error-free of billing and other documentation processes in maritime transport, either with shipping lines, freight forwarders/NVOCCs or port operators, are considered by service buyers as an element of service quality, as well as a criterion for carrier/port selection. With security improvements, this quality attribute can be enhanced substantially. Indeed, while integrated IT and EDI systems are necessary inputs for security requirements, it is not hard to see that such systems in place would also facilitate the documentation processes of maritime transport service providers, in which information regarding shipment, operations, etc. can be effectively relayed from service buyers to service providers and among service providers without manual input. Thus, such systems help to reduce the intervention of human input and possible errors in the processes of documentation preparation and issuance. In this respect, security improvements are a catalyst for enhancing the reliability of documentation as a service quality attribute in maritime transport.

Another potential impact of security improvements is on the competitive price of service. The infrastructure and facilities of transport have long been designed and built for efficiency and competitiveness, not security. In maritime transport services, specifically, the competitive price of service is critically important as the profit margin in this sector is very slim. Security improvements such as investments in the adjustment of the current IT and EDI systems, technological solutions and other security-related processes and procedures required by security initiatives would affect the operating and capital budgets of many firms, especially the small and medium-size ones in developing countries, and therefore increase the cost of providing the service. The impact of security improvements on the price of maritime transport services can be viewed from two perspectives: (1) security improvements would lead to an increased price of service and therefore affect the competitiveness of the service provided. While the security requirements of some initiatives, such as the ISPS Code, are quite obviously compulsory to targeted maritime organisations of all member countries, small and medium-size companies will find bearing the costs associated with these requirements more difficult than companies with greater resources. In other words, the impact would be greater for small and medium-size maritime transport service providers, for whom the costs associated with security improvements can be proportionately greater and easily erode their slim profit margin and competitive price of service provided. One can argue that costs of security improvements can be considered a major investment, just like quality, which, in the long term, will result in benefits, including competitive price of service.

While security improvements are perceived as having a positive impact on some quality factors, it can also be argued that this positive impact can be jeopardised by the cost and management factors. Costs of security improvements are still the main hindrance for many

small and medium-size maritime transport service providers, especially in developing countries like Vietnam. The cost factor can be viewed from two angles. Firstly, the costs of security investments in IT, EDI and technological solutions can well be a burden to companies which do not have enough resources. In the long run, however, benefits should outweigh the initial costs of security investment. Secondly, the costs of ineffective security management may be larger than the potential benefits realised from security improvements. In this respect, the management factor is critically important. An 'examine everything' inspection approach or bad management of shipment information, for instance, can potentially lead to delays and congestion, and thus reduce the speed and reliability of service.

Improvements following security requirements potentially may also be beneficial to maritime transport service providers by supporting their quick response to customer inquiries, better knowledge of the businesses and the needs of their customers, as well as enhanced application of IT and EDI in customer service. Indeed, if the service providers in maritime transport have integrated IT and EDI systems in place, as well as technological solutions for better control of shipment visibility, benefits will be realised not only in enhanced security protection but also in improved capability of service providers in knowing and responding to their customers' needs and requirements. Wolfe (2002) argued that the ability to recognise and react early to problems, thanks to better shipment visibility, increases operational flexibility. Shippers and carriers can respond more effectively to changes. The AIS transponder on board vessels following ISPS Code requirements, for example, can enhance visibility control between ships and organisations ashore. Furthermore, the application of integrated IT and EDI systems in organisations, as a by-product of security improvements, can provide them with the capability to better conduct

Customer Impact Management (CRM) with data mining supported from such systems. Organisations can also enhance their service functions such as on-line customer support services by the application of IT and EDI systems in place. However, again, this impact may be constrained by the cost factor of initial security investments. For small and medium-size companies especially in developing countries, the costs of initial security investments are still the main hindrance in recognising the long-term benefits resulting from security improvements. Nevertheless, the trend towards business operating practices with integrated IT and EDI systems is inevitable and it is expected that maritime transport service providers will soon realise the benefits of such systems in their organisations, not only from the business operations perspective but also from the viewpoint of security improvements and their impact on organisations' capability to better manage the impact with their customers.

Security improvements impact on the efficiency of operations and the management of maritime transport service providers. This is, perhaps, the most concerning aspect of the impacts between security and service quality in maritime transport operations. A review of the literature in this respect identified several discussions on the impact of heightened security on the efficiency gains of the supply chain. The main focus was on the negative impact of reactive security measures which can lead to adverse impacts on JIT practices. More specifically, these measures may jeopardise the long established efficient business operating practices which have brought massive efficiency gains to the global supply chain. Indeed, if security is not effectively managed and an 'inspect everything' practice is utilised, the efficiency of operations and management of supply chain players, of which maritime transport service providers are a key partner, may deteriorate. The efficiency of an integrated supply chain may be put at some risk because it is no longer prudent to optimise operations so completely around cost minimisation (Wolfe 2002). Another example of the importance

of proper management of security is White's (2003) study of container inspection as required by CSI at transhipment ports. By using mathematical modelling to minimise the number of inspection and transhipment container moves, it was found that the list of container inspections is important to port efficiency, since the ship's departure time is highly variable if this list is submitted after the ship has docked.

There is still room for improvements in efficiency of operations and management in maritime transport, especially when the level of IT and EDI utilisation is limited. Investments in these integrated systems and other technological solutions, together with some required changes to operating processes and procedures in line with security requirements, would result in potential benefits for maritime transport service providers both in terms of security and efficiency of operations and management. In shipping companies and freight forwarders/NVOCCs, the enhanced capability of service providers in shipment visibility control, increased speed of service performance, and reliability of service performance and documentation processes can enhance the efficiency of their operations and management. They also help to enhance efficient information exchange at the ship/port interface, as well as among partners in the integrated supply chain. Overall, they help the maritime transport service providers to reap efficiencies in their operations and management. For example, Basil Maher, president and CEO of Port Elizabeth, NJ-based Maher Terminals Inc., sees the possibility of improved training, pre-screening of inbound containers on foreign soil and other initiatives contributing to—rather than detracting from—expedient operations. He argued that training of employees in security-related issues should help move non-threatening boxes faster, while better pinpointing those containers that require greater scrutiny, and as such, heightened security efforts could actually enhance efficiency of container terminals (Abbott, 2002).

All of the impact discussed earlier would help to create a better image of maritime transport service providers, as their reputation for reliability in operations and management can be further enhanced by security improvements. According to Eyefortransport (2002), the early targeting of high-risk containers as required by the CSI initiative is potentially of great value to the ports that have implemented heightened security initiatives, since they will become more attractive locations to those companies that depend on timely movement of merchandise or processing inputs. The reputation for reliability of maritime transport service providers enhanced by security improvements, however, may be jeopardised by the ineffective management of security requirements or efforts. It has been argued earlier that if the management of security improvements is not effective, they can easily lead to adverse impact and therefore negatively affect the efficiency and reliability of business practices in maritime transport operations. Heightened security processes and procedures without proper profiling of security risk magnitude, for instance, can result in possible delays.

Maritime security threats, such as piracy or terrorism, have been perceived as potential dangers for safe maritime transport. Improvements in maritime security, in terms of enhanced security awareness in the business environment, assist the socially responsible behaviour and concern for human safety of maritime transport service providers. In practice, the issues of safety and environmental protection in maritime transport are closely linked with each other. Improvements in security would also have the potential to increase awareness and concern of maritime transport service providers about environmental protection. The proposition that security improvements would enhance social responsibility, as a quality dimension of maritime transport services, may be debated from two perspectives. From the social perspective, the more security improvements are made, the

better, since society would benefit from more secure shipping, and from safety and environmental protection concerns being considered by all maritime transport service providers. The Taguchi Loss Function model (Taguchi, 1924) in relation to quality cost can be applied to explain society's expectation regarding security improvements in maritime service organisations, since such improvements would lessen the cost to society of safety and environmental accidents. From the standpoint of maritime transport service providers, however, excess security efforts for the perceived level of security threat, or ineffective management of security improvements, may lead to waste for organisations and negative impact for society. Good management of security improvements therefore becomes critical to maritime transport service providers to help them achieve their business objectives and to be 'good citizens' at the same time.

To summarise the discussion above, Figure 1 depicts the framework of projected impacts of security improvements on various aspects of service quality in maritime transport.

Insert Figure 1 about here

METHODOLOGY

Research question

This study aims to examine whether there are impacts of security improvements on quality of maritime transport service, and how they are described. There is little literature about these impacts and they have not been empirically tested for validity. Logical deduction, however, suggests that these impacts exist.

Methods of data collection

Triangulation is utilised in this study. Triangulation is strongly suggested in transportation and logistics research literature as an effective and useful technique to achieve the width and depth of research issues, as demonstrated in the study by Cunningham et al. (2000). The type of triangulation technique employed in this paper is the methodological triangulation, in which the author used and combined quantitative and qualitative methods to obtain a comprehensive understanding and a wide and deep picture of the research question. The methods of data collection and interpretation used in this study are the survey method (by using mail questionnaires) followed by confirmatory in-depth interviews.

Sampling design

The sampling frame for this research is constructed from the directory of shipping companies, port operators and freight forwarders/NVOCCs in Vietnam listed in the Visaba Times—Vietnam Shipping and Logistics Review. A list of 197 maritime transport service-providing organisations including 66 shipping companies, 49 port operators and 82 freight forwarders/NVOCCs, is used as the mailing list for this research. By the cut-off date, 119 questionnaires were returned, of which 42 were from shipping companies, 43 from port operators, and 34 from freight forwarders. This represents a 60% overall response rate.

For in-depth interviews, the same population and sampling frame was used as for the survey. The process of selecting the samples for interviews was conducted carefully. First, the samples for interviews were chosen only from within the respondents to these surveys. Secondly, since the research population consisted of three categories of service providers, it was important that the sample chosen for qualitative research also reflected the representativeness of these categories. Geographical representativeness of the sample was also assured. As the shipping companies, port operators and freight forwarders/NVOCCs

were located all over the North, Central and Southern regions of Vietnam, the sample selected for in-depth interviews also covered organisations in all these three regions. With these considerations in mind, 25 in-depth interviews were conducted during the study period.

Design of research instruments

Both fixed-alternative and open-ended response questions were utilised in the questionnaire, preceded by a cover letter. There were three main questions in the questionnaire following closely the format depicted in Figure 1. In the first question, respondents were asked to indicate their attitude on a five-point Likert scale, starting from 1 as 'strongly disagree' to 5 as 'strongly agree', to the statement that "changed operating practices following security improvements could lead to the enhancement of various service quality factors". The second question was similar to the first, asking respondents' attitude toward the statement that "enhanced security awareness as a result of security improvements would lead to the enhancement of environmentally safe operations and socially responsible behaviour and concern for safety as other service quality factors in maritime transport". The third question was an open-ended one, asking respondents to elaborate on their arguments if they had indicated a negative attitude to the statements in the earlier two questions. The questionnaire was written in English and translated into Vietnamese. To ensure that the translation of the instrument in the target language was equivalent to the original language in which the instrument was developed, the process of translation of survey instruments was conducted through the consecutive stages of forward translation (English to Vietnamese), pre-testing (for both English and Vietnamese versions), modified translation (with feedback from instrument pre-testing), backward translation (modified Vietnamese version to English), and finalisation of Vietnamese version (based on comparison between backward translated English version and the original one).

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

The mail survey and in-depth interview questionnaires are shown in the Appendices.

Administering mail survey and conducting in-depth interviews

The questionnaire was pre-tested with a group of 10 organisations. Once this was completed and all feedback was incorporated in a revised questionnaire, the Vietnamese version was mailed, together with a cover letter and a self-addressed envelope.

Prior to the interviews, a list of prospective interviewees in various organisations was drawn up, and each of these interviewees was contacted by telephone inviting their participation in the interviews. The list of prospective questions was also forwarded to those who agreed to participate in the interviews. The interviews were conducted on a one-to-one basis and

averaged approximately forty-five minutes. A tape recorder was used to record the whole interview with the prior consent of the interviewees.

RESEARCH FINDINGS

Survey respondents' attitude toward projected impacts

Table 1 shows the explanation of codes of variables used in the mail survey. Each variable represents a projected impact in the research framework.

Insert Table 1 about here

Descriptive statistics and the Chi-Square test for goodness-of-fit were the tools of statistical analysis employed to shed light on perceptions of the 13 projected impacts. Mean and standard deviations were computed to provide a general descriptive profile of the variables. Based on the mean scores, conclusions could be drawn from survey respondents' perceptions of whether a projected impact will actually exist. Specifically, as the midpoint of the scale is 3 (neutral), those variables having a mean score greater than 3 would indicate that the impacts are supported by the survey respondents. Furthermore, Chi-Square test for goodness-of-fit was used to test the null hypothesis that there is no significant difference between observed and expected values of the sample frequency distribution (Zikmund, 2003). In this respect, if the computed asymptotic significance value (*p* value) of each variable is smaller than 0.05 (selected probability level) the null hypothesis is rejected. Thus, it could be then concluded that the difference between observed and expected values of the sample frequency distribution is not due to chance variation. Table 2 shows the results of the descriptive statistics and Chi-Square test on respondents' perception of projected impacts of security improvements on service quality factors.

Insert Tables 2 about here

It can be seen from Table 2 that all the variables have mean scores greater than 3 and p values smaller than 0.05, implying that survey respondents support and agree with all the projected impacts of security improvements on service quality factors. Among the projected impacts, respondents show the highest level of consensus for the idea that changed operating practices, including security-related investment in IT and EDI, can lead to enhancement of wider application of IT and EDI in operations and customer service (COPSQ9). This projected impact has the highest mean score. The second most agreed upon projected impact is that enhanced security awareness in the business environment, as part of security improvements, would lead to enhancement of the organisations' socially responsible behaviour and concerns for human safety (SEASQ1). Respondents also showed a high level of consensus on the projected impact that changed operating practices, including IT and EDI investment, would enhance the reliability of documentation (COPSQ5).

The positive impact of security improvements, specifically, enhanced security awareness in the business environment enhancing perceptions of the organisations' social responsibility is again confirmed. In this connection, respondents agree that organisations would increase their environmentally safe operations in line with enhanced security awareness as a consequence of security improvements (SEASQ2). On the impact of changed operating practices, including security-related IT and EDI investment on shipment safety and security (COPSQ4), respondents also showed a high level of consensus, with the response mean score of 4.33. Security improvements in terms of changed operating practices, including security-related investment in IT and EDI, also impact on the organisations' image through its enhanced reputation for reliability in the market (COPSQ11). Respondents believe that security improvements, through their positive impact on timeliness of shipment pick-up and delivery, shipment safety and security, and reliability of documentation, would help to

enhance the organisations' image as reliable service providers. Respondents also agree that investment in IT and EDI, as part of security-related improvements, would enhance the service providers' capability in shipment tracing (COPSQ1).

The impact of security improvements, in terms of changed operating practices including security-related IT and EDI investment, on the organisations' efficiency in operations and managements (COPSQ10) is a projected impact which receives average consensus from survey respondents (mean score = 3.82). Similarly, the projection that changed operating practices including security-related investment in IT and EDI would enhance the speed of service performance (COPSQ2) has an average mean score of 3.75. Another projected impact of security improvements on service quality factors is between changed operating practices, including IT and EDI investment, and the timeliness of shipment pick-up and delivery, or the reliability of service performance (COPSQ3) with the mean response of 3.72.

Survey respondents also expressed mixed responses to the projection that changed operating practices, including security-related investment in IT and EDI, would make the organisations' price of service competitive in the long run (COPSQ6). This has a low mean score of 3.63. Lastly, respondents express the lowest level of agreement with the projection that if service providers changed operating practices including security-related investment in IT and EDI in the organisation's operations, they would have better knowledge of customers' needs and requirements (COPSQ8). This projected impact has a low mean score of 3.48.

Another observation from Table 2 is that, among the 13 projected impacts of security improvements on service quality factors, there are seven projections in which the mean responses are greater than 4 (indicating agreement), the other six having a mean response of less than 4 but greater than 3 (indicating a neutral attitude). From the general perspective, it is quite evident that there are positive impacts of security improvements on service quality factors as perceived by the survey respondents in that the former will enhance the latter, since all the mean responses to these projections are above the midpoint of the scale. Nevertheless, from the critical perspective, these impacts are reflected as completely positive (with mean responses greater than 4) for the following projections:

- Changed operating practices following security requirements lead to the enhancement of wider application of IT and EDI in operations and management.
- Increased security awareness would enhance socially responsible behaviour and concerns for human safety.
- Changed operating practices following security requirements lead to the enhancement of reliability of documentation.
- Increased security awareness would enhance environmentally safe operations.
- Changed operating practices following security requirements lead to the enhancement of shipment safety and security.
- Changed operating practices following security requirements lead to the enhancement of the organisations' reputation for reliability in the market.
- Changed operating practices following security requirements lead to the enhancement of shipment tracing capability.

Interviewees' attitude toward projected impacts

There are mixed responses among the interviewees regarding attitude to and perception of the projected impacts. In this connection, some interviewees perceive that security improvements, including security-related IT and EDI investment, as well as compliance with other security requirements like the ISPS Code, would definitely have positive impacts on service quality. Others argue that such security improvements only result in difficulties for the organisations' operations and management and thus negatively affect service quality. Nevertheless, most of interviewees felt that although there are some negative impacts of security improvements on service quality, they are outweighed by the positive ones.

One of the main points some interviewees used to support their argument of the negative impact of security improvements on service quality is that these requirements and improvements only create an extra workload for service providers, as they have to spend more resources, both in monetary and labour terms, to comply with the new requirements. Others argued that such activities are unnecessary before the security issue is raised, thus such security requirements will only create a burden for them. From another perspective, some interviewees argued that security requirements need large investment costs and can only lead to shipment delays in the transport chain, thus negatively affecting service quality. A typical comment of a ship operator illustrates this.

> … in my opinion, when there is the need for security it is obvious that it incurs additional large costs for the company to invest on IT and EDI system following security requirements… These requirements do not improve service quality, because in terms of time they cause delay for shipments. If there is no terrorism, these requirements are just a burden for shippers, consignees and transport service providers in terms of time and money…

Another interviewee, while acknowledging that security requirements may be good for management since the crew may feel that they are more strictly managed under the new security requirements and thus will be more observant, also believed that this will create more pressure for crew and increase their workload. He felt that this will lead to negative results since the organisation may focus too much on compliance with security requirements and neglect other main business objectives. Conversely to the above, other interviewees strongly argued that these impacts are, in fact, only good and positive for service providers' service quality. They argue that security-related investment in IT and EDI have benefits not only for security purposes but also for other business improvements, such as operations and management. Therefore, the impact of such investment on service quality is only good as it helps to improve the outcomes of service performance, such as increasing the reliability of information by reducing human errors and input. Regarding other security improvements such as the introduction and application of the ISPS Code, interviewees also argue that these requirements have formalised the need for security in maritime transport, and are applied to not only terrorism but also other traditional security threats such as piracy, cargo theft, etc. The impacts of such requirements on service quality would be positive since they act as a catalyst for other good changes in management and enhance the organisations' image in the market. A ship operator comments on this as follows:

> …I think the investment in IT and EDI are not only for security improvement, especially after the September 11th event, but also for other business objectives, including service quality enhancement… They help to decrease the costs of inputs and thus the price of service as the output to attract customers… First, IT and EDI help companies control the process of service performance, for instance, management can now communicate and consult with their ships while they are at sea in order to make the voyages safe and efficient. Secondly, they make the transactions with ports, customers, management and staff faster and more efficient as well… It is noticed that the security requirements for ships and ports are not only for countering terrorism, but also for enhancing the efficiency of

> service quality… They also help to enhance the management capability for staff, and standardise the management practices following common requirements in the international codes and regulations. It is obvious that port and ship security is not only for security purpose but also for improving and standardising the operation and management capability in maritime transport, thus enhancing service quality…

Many interviewees realise that security improvements, with the introduction of some new security requirements, have played a key role in enhancing awareness about security in organisations. It was argued that improvements such as compliance with the ISPS Code, would enhance the organisations' image of reliability in the market, and restore confidence for customers, while not jeopardising the smooth and efficient flow of cargo. It was also argued by some other interviewees that security improvements, in terms of investment in IT and EDI systems and other requirements such as compliance with the ISPS Code, will equip the organisation with much better knowledge about contemporary security threats. This would help them better prepare to assure security and thus not negatively affect other business objectives, including service quality. One of the main arguments in this respect was that international trade is more and more complex, and so are the security threats in maritime transport. Some interviewees pointed out that, in the past, issues in maritime security were in the form of piracy, cargo theft, stowaways, etc., but now there is even more sophisticated theft and fraud via the world wide web. Without being equipped with security information and knowledge through these security improvements, it is possible that organisations would suffer losses, in terms of security and service quality as well.

Beyond these views on the impacts of security improvements on service quality, the majority of interviewees agree that there are both negative and positive impacts, but that the latter would outweigh the former. In this connection, the interviewees' consensus on the negative

and positive impacts of security improvements on service quality is basically similar to what has been agreed upon by other interviewees who simply either criticise or support the projected impacts. Specifically, it was commonly argued in the interviews that improvements following security requirements would incur additional costs for the service providers, and create more workload for staff, thus affecting the outcomes of service performance. Nevertheless, it was also contended that such changes following security requirements would result in benefits that exceed the disadvantages, since they motivate the organisations to change current operating practices to incorporate better planning, thus enhancing reliability and management efficiency of service performance. In the meantime, interviewees argued that the benefits brought about by security improvements would far offset the initial costs of investment on equipment, facilities and information systems, as they help to create a better image for the organisation thus attracting more business in the long run. More importantly, such security improvements would enhance security awareness, and facilitate an organisation's sustainable business development. This is illustrated by a ship operator who states that 'the most visible impacts of security can be seen in information security and assurance of customer data, and with the information system the firms will have more advantages in their business processes'. In fact, these positive impacts of security improvements on service quality are perceived not only in terms of IT and EDI investment, but also from other improvements following security requirements such as compliance with the ISPS Code. In this connection, interviewees argue that such requirements do not actually slow the operation process down, but conversely enhance the company's image and assure the safety and security of their equipment and facilities as well as their customers' cargo. A ship operator elaborates on this as follows:

> …It was usually not possible to control the people going on board and ashore, especially in foreign ports. With the application of the ISPS Code, those people have to wear badges, and our ship security

> officers can control them easier than before. First, the company feels more secure, and secondly, it creates a professionalism that everybody can realise from such practices. So I think they will help to enhance the image of ships as well as the company, and thus do not hamper service quality…

Acknowledging that security improvements may be perceived as a hindrance to business practices as they require some current practices to be changed, new ones to be implemented and some companies may feel irritated about this, many interviewees still affirm that this feeling will be soon replaced by the confidence vested in them. The main argument for this is that better preparation and planning right from the beginning will protect the organisation from losses that they may incur downstream. Security, like the issue of quality, should be viewed through a holistic perspective, and that it will pay back in the long run. While the factors assumed to be negative impacts—such as initial cost of investment, increased workload, etc.—are visible, the positive impacts of security improvements on service quality are somewhat invisible but have intangible benefits and advantages for the organisation in the long run. One of the benefits seen through the interviews is increased customer satisfaction with the improved service performance and reliability. Again, it is the company's image and enhanced security awareness that is most visibly perceived with security improvements. A port operator confirms this as follows:

> … Security requirements require big investments, for example some big ports require container scanners, camera, etc. However, if the port is not concerned about security investment, customers, especially foreign shipping lines, may consider the port as not safe and secure, thus reducing the business to the port. Although the initial investment may be substantial, I consider that is necessary since the port will become safer and more attractive to shipping lines and cargo owners…

While appreciating the positive impacts of security improvements on service quality and believing that the advantages brought about by these improvements will outweigh the

disadvantages, interviewees also clearly argue that the management of security practices should be effective to minimise the costs and maximise the benefits. This requires knowledge of critical success factors for the effective management of security so as to ensure security while enhancing business performance. The following quote best describes how effective security management is important to make security a part of the daily business and contribute to its success:

> …Security improvements, in my opinion, are to add more workload for operations as well as management. So it is clear that if security management is not effective, it will become a hindrance to business processes. However, it is also obvious that without security improvements, ineffective management can cause hindrance as well, and vice versa, good management will not cause any hindrance although all security improvements have to be conducted… Security requirements create some burden of investment following requirements from conventions, but to effectively manage them is just a matter of good management from current work practices…

In short, all projected impacts between security improvements and service quality are supported by both survey respondents and interviewees. The statistical analysis reveals that, among the 13 projected impacts, respondents indicate clear consensus of agreement on seven projections, in which security improvements can enhance service quality in terms of increased reliability of service performance, social responsibility awareness, increased efficiency in operations and management, as well as enhanced image in the market. For the other projections, the respondents' agreement is not clearly shown. This is also reflected in interviewees, where respondents emphasise the most notable benefits brought about by security improvements in terms of increased reliability of service performance, increased awareness and better image, thus positively affecting customers' perception of the organisation's service quality. In this respect, this study showed that although there are some disadvantages, what security improvements can bring about for service quality and business

success is greater than the disadvantages, and is critically needed for long-term business sustainability.

CONCLUSION

This paper empirically reveals that security improvements result in positive impacts on service quality, specifically that changed operating practices following security requirements, as part of security improvements, would lead to wider applications of IT and EDI in operations and customers service, increased reliability of documentation, enhanced shipment safety and security, enhancement of the company's reputation for reliability in the market, and shipment tracing capability. The other positive impacts are that enhanced security awareness in the business environment, as part of security improvements, would result in enhanced socially responsible behaviour and concern for human safety, as well as an increase in environmentally safe operations. However, service providers in maritime transport must employ effective security management strategies, and this has an implication as one of the new challenges in modern shipping.

REFERENCES

Abbott, P. S. (2002). Security could enhance efficiencies. *The American Journal of Transportation On-line*, http://www.ajot.com/scripts/foxweb.exe/ajotweb.exe?2,2863.

Aichlmayr, M. (2003). Can technology prevent disaster?. *Transportation & Distribution*, **44(1)**: 50–53.

Cunningham, L., Young, C. & Lee, M. (2000). Methodological Triangulation in Measuring Public Transportation Service Quality. *Transportation Journal*, Fall: 35–47.

Eyefortransport (2002). Cargo security overview: Technologies, government and customs initiatives. http://www.eyefortransport.com/index.asp?news=33800&ch=159.

OECD (2003). Security in maritime transport: Risk factors and economic impact. http://www.oecd.org/dataoecd/19/61/18521672.pdf.

Sennewald, C. A. (1978). *Effective security management*. Butterworth: USA.

Taguchi, G. (1924). *Introduction to quality engineering: designing quality into products and processes*. Asian Productivity Organisation: Tokyo.

White, C. (2003). Maritime security: Challenges in supply chain management & design. In: Proceedings of International Maritime and Port security conference, Singapore, http://www.isye.gatech.edu/setra/reports/impscJan03.pdf.

Wolfe, M. (2002). Freight transportation security and productivity: complete report. http://www.nutc.northwestern.edu/sources/FRT/SEC/Wolfe_FrtTransSecProd_0402.pdf.

Zikmund, W. G. (2003). *Business Research Methods*. 7th edition. Thomson Learning, South-Western Publishers: USA.

FIGURES AND TABLES

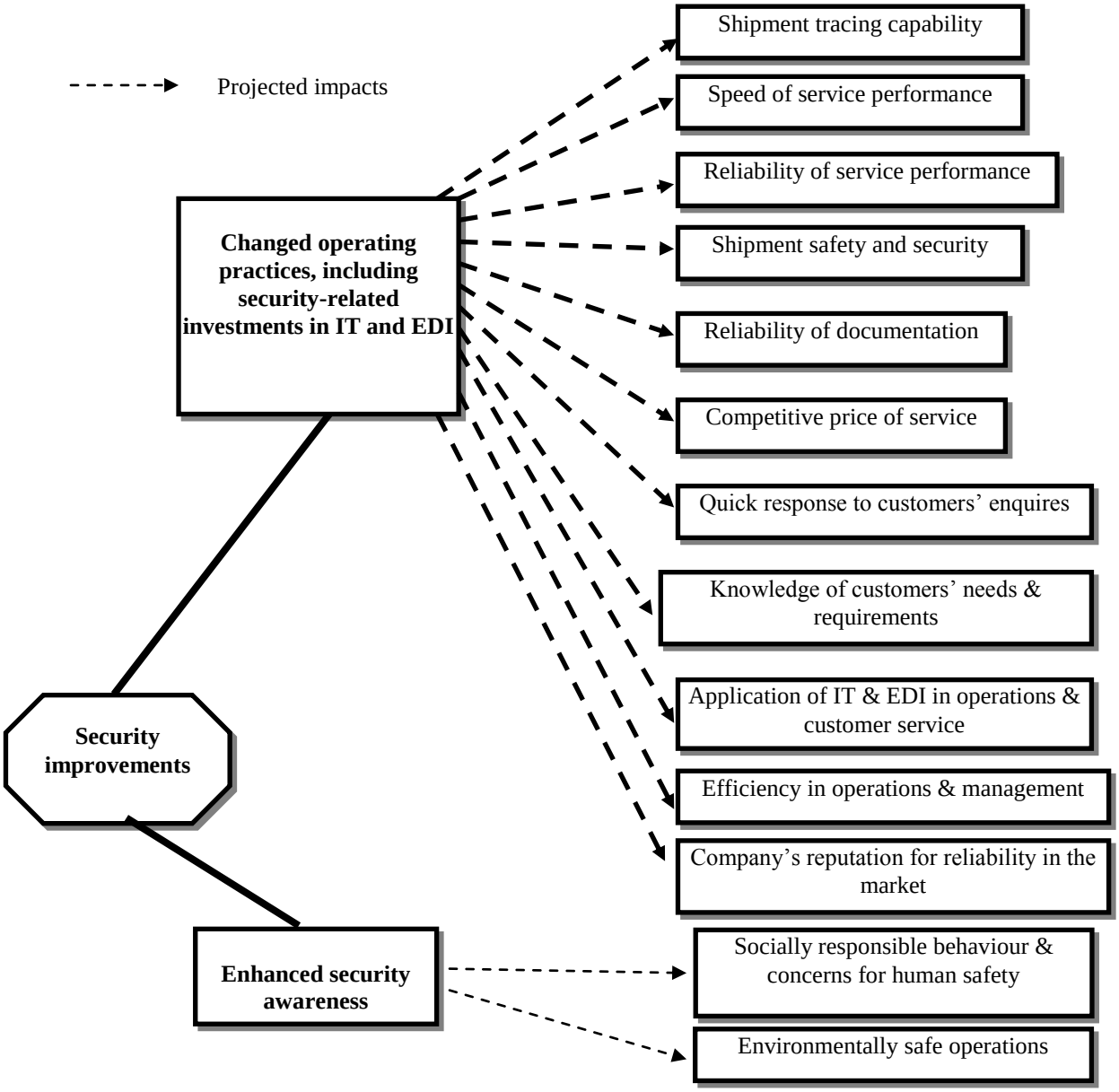

Figure 1: Projected impacts of security improvements on service quality factors

Variable (projected impact)	Code
Changed operating practices including security-related IT and EDI investment lead to the enhancement of:	
Shipment tracing capability	COPSQ1
Speed of service performance	COPSQ2
Timeliness of shipment pick-up and delivery	COPSQ3
Shipment safety and security	COPSQ4
Reliability of documentation	COPSQ5
Competitive price of service in the long run	COPSQ6
Quick response to customers' enquiries	COPSQ7
Better knowledge of customers' needs and requirements	COPSQ8
Wider application of IT and EDI in operations and customer service	COPSQ9
Efficiency in operations and management	COPSQ10
Enhanced company's reputation for reliability in the market	COPSQ11
Enhanced security awareness leads to the enhancement of:	
Socially responsible behaviour and concerns for human safety	SEASQ1
Environmentally safe operations	SEASQ2

Table 1: Explanation of codes of projected impacts of security improvements on service quality factors

Variables	Mean	Std. Deviation	Chi-Square statistics	Chi-Square p value	Degree of freedom
COPSQ9	4.58	0.59	60.12	0.000	2
SEASQ1	4.53	0.53	55.78	0.000	2
COPSQ5	4.43	0.65	35.41	0.000	2
SEASQ2	4.35	0.56	50.49	0.000	2
COPSQ4	4.33	0.69	23.21	0.000	2
COPSQ11	4.07	0.61	48.02	0.000	2
COPSQ1	4.06	0.63	40.15	0.000	2
COPSQ10	3.82	0.74	9.60	0.008	2
COPSQ2	3.75	0.74	13.38	0.001	2
COPSQ3	3.72	0.76	52.73	0.000	3
COPSQ7	3.65	0.72	66.18	0.000	3
COPSQ6	3.63	0.66	77.54	0.000	3
COPSQ8	3.48	0.64	97.91	0.000	3

Table 2: Perception of projected impacts of security improvements on service quality factors

Note: mean scores computed on 5-point scale; 1 = strongly disagree, 5 = strongly agree

APPENDIX 1

STUDY OF SECURITY MANAGEMENT IN MARITIME TRANSPORT INDUSTRY

General guidance

1. *This questionnaire contains two parts. Part A is about the impacts between security improvements and service quality, part B asks general questions for classification.*
2. *Responses will not be associated with individual respondents; only summarised information will be included in the report.*
3. *If you have any questions, please feel free to call: Thai Van Vinh, Australian Maritime College, Tel.: +61 3 6335 4764 or Email: V.Thai@ amc.edu.au*
4. *'Security' in the context of this study should be understood as the framework of security policies, processes, procedures and technology employed to protect the maritime transport service providers from maritime security threats (piracy, armed robbery, stowaways, cargo theft/pilferage, drug/people trafficking, information security and maritime terrorism), which can endanger their resources (properties, human resources and information) and services provided, as well as responsibilities to their stakeholders.*
5. *'Security requirements' imply the requirements imposed by regulations such as the ISPS Code and other international and national regulations, as well as the internal requirements for security within the organisation, to ensure 'security' as elaborated above.*
6. *'Changed operating practices' refer to operation processes and procedures that have been changed to comply with security requirements, such as early and electronic submission of shipment information, transparent shipment data, etc.*

A. SECURITY IMPROVEMENTS AND SERVICE QUALITY

I. Please indicate your view on the following statements, by rating them, where

1 = strongly disagree 2 = disagree 3 = neutral 4 = agree 5 = strongly agree

1. Changed operating practices following security requirements, including security-related investments in IT and EDI in the organisation's operations, can lead to the enhancement of:

a	Shipment tracing capability	1	2	3	4	5
b	Speed of service performance	1	2	3	4	5
c	Timeliness of shipment pickup & delivery	1	2	3	4	5
d	Shipment safety and security	1	2	3	4	5
e	Reliability of documentation	1	2	3	4	5
f	Competitive price of service in the long run	1	2	3	4	5
g	Quick response to customers' enquiries	1	2	3	4	5
h	Better knowledge of customers' needs & requirements	1	2	3	4	5
i	Wider application of IT & EDI in operations and customer service	1	2	3	4	5
j	Efficiency in operations and management	1	2	3	4	5
k	Enhanced company's reputation for reliability in the market through (c), (d) and (e)	1	2	3	4	5
l	Others (Please specify)					

2. The enhanced security awareness in business environment leads to the enhancement of:

m	Socially responsible behaviour and concerns for human safety	1	2	3	4	5
n	Environmentally safe operations	1	2	3	4	5

II. If you answer 'strongly disagree' or 'disagree' to any of the above statements, please elaborate in the space given below or attach another page if necessary.

_____

_____

_____

B. PERSONAL INFORMATION

1. Please indicate (*by checking the box*) the business sector in which you are working:

   Shipping company ☐ Port operator ☐ Freight forwarding company ☐

2. What is your title: _____
3. Your experience (in years) in this industry: _____
4. Do you wish to receive (*by checking the box*) the summary of results?

   Yes ☐ *No* ☐

Should you wish to receive the summary of results, please provide your postal or email address (this will not be revealed to anybody).

_____

_____

THANK YOU VERY MUCH FOR YOUR PARTICIPATION

APPENDIX 2

INTERVIEW QUESTIONNAIRE

1. Do you think improvements of security, such as security-related investments on IT and EDI, will have impacts on any service quality factors in your business sector? Will they be positive or negative and how?
2. What will be the impacts of security requirements on the service quality-related factors in your business?