

Critical success factors of effective security management: a survey of Vietnamese maritime transport service providers

VINH Thai-Van, Devinder GREWAL

School of Maritime Management & Logistics, Australian Maritime College, Tasmania, Australia

Abstract

In this study, based on the analysis of the nature of security threats, we place the three corner stones for the effective management of security in maritime transport: quality management (QM), risk management (RM), and business continuity management (BCM). A conceptual model of critical success factors of effective security management is devised following this reasoning. The model is further analysed and discussed following the analysis of a survey conducted among three main groups of maritime transport service providers in Vietnam: shipping companies, port operators, and freight forwarders/NVOCCs towards this research issue. Findings from the survey proved that all proposed 24 critical success factors are valid and should be used as critical factors for success in effectively managing security in maritime transport, so as to satisfy security requirements while enhancing other business objectives. The confirmed implication of this research is that effective security management can be achieved by employing critical success factors derived from the fundamental principles of quality, risk and business continuity management.

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

1 Introduction

In recent years, the issue of maritime security has become a major concern on the international maritime agenda. Maritime security dates back to early maritime history under the themes of piracy and cargo theft and now includes also stowaways, people and drug trafficking, information security and, of course, maritime terrorism after the September 11th event. There have been some arguments elsewhere that heightened security measures would hamper international trade and have negative impacts on business results. However, from the management point of view, security threats in maritime transport should be viewed

as one of the risks in the organisation's risk profile. The objective of security management is to support the organisations in achieving their business goals and objectives. The management of security in maritime transport is therefore, in fact, a management and business issue rather than the compliance with international security conventions. With this background, one of the fundamental questions in security management is how to achieve effective security management, e.g. satisfying security requirements while enhancing other business objectives, such as service quality or operational efficiency. In other words, it is important to identify and comprehend the critical success factors (CSFs) for the effective management of security in maritime transport. In this paper, we aim to seek the answer to that question. The remainder of this paper is organised as follows. First, the fundamental background for this research is presented in that three approaches to effective security management are analysed and discussed. Based on this, the critical success factors (CSFs) of effective security management are identified. Empirical validation of these CFSs is presented next with the research methodology described and findings discussed. The paper concludes with recommendations for future extension of this research.

2 Fundamental background

2.1 The QM approach to effective security management

2.1.1 Security design and process control

In quality management, in-process quality control and management is needed as a supplementary philosophy to prevent it from the source so as to ensure that variability during the process is driven out. Similarly, the prevention from the source in security management must be followed by in-process control in order to monitor shipments while they are in transit and thus significantly reduce the risks of a shipment being tampered with, creating security breaches. In this respect, the primary objective of process control in the management of supply chains and maritime transport security is to have a better visible control of shipments while they are en route, so as to ensure the integrity of physical shipments and their associated information. A quality system like Poka-Yoke can be effectively applied to security management so that operating processes of shipment movements can be controlled and managed for security purposes. These processes must be designed and built in so that any tampering of the shipments has to be detected, and mitigation measures are immediately deployed in due time. Like quality, security should be built in from a project inception. Besides, security should be integrated into the overall business policy and plans and should not be conducted as a separate issue. This approach to security management will help make security accepted as part of the daily business operations.

2.1.2 Total organisational focus in security management

In quality management, it is seen that the total organisational focus in terms of the commitment and leadership of senior management, and the involvement, empowerment and training of employees is crucial so as to inspire a quality culture throughout the organisation, thus contributing to improved quality. The bottom line in this respect is that senior management realises that the long-term benefits of quality far exceed the costs of conformance. Security, as it is traditionally defined

in organisations, is one of the most pervasive problems that an organisation must address. Since security is a problem for the whole organisation, it simply is no longer effective or acceptable to manage it from a security department. Quality initiatives such as the Six Sigma process emphasise the awareness, focus, and dedication of everyone in the organisation to identifying and fixing quality problems, and such a total approach is what is needed in addressing security problems; Lee and Whang [1]. In fact, since the support by senior management for improving the quality of products and services is already in place in many organisations, what is important is that management executives realise the eventual return on their security investment in the form of greater efficiencies, better contingency planning against disruptions and improved levels of customer service Doak [2]. Like quality, the key to success in implementing security measures is the commitment and support from senior management so as to inspire the security culture throughout an organisation, thus promoting the involvement and empowerment of all employees in security matters. In this respect, teamwork is also critical, and people must work together to get security work done since no one person can secure a business. Like in quality management, the total organisational focus in security management is vital for the success of any security program. This total approach must start with the commitment of senior management and their security leadership, followed by the empowerment and involvement of all employees, supported by sufficient training in security matters.

2.1.3 Continuous security improvement cycle

Continuous improvement has been proved to be fundamental for success in quality management, especially in TQM. Since quality improvement is a process, organisations should strive for continuous efforts so as to drive all the variables out of the process and achieve a 'zero defect' quality goal. Together with the Six Sigma cycle, the PDCA (Plan-Do-Check-Act) cycle, commonly known as the Deming cycle, forms the conceptual basis of continuous improvement activities in many companies; Deming [3]. Since security is a process and not a product, the same approach should also be taken to effectively manage security, meaning that organisations have to strive for continuous security improvement (CSI).

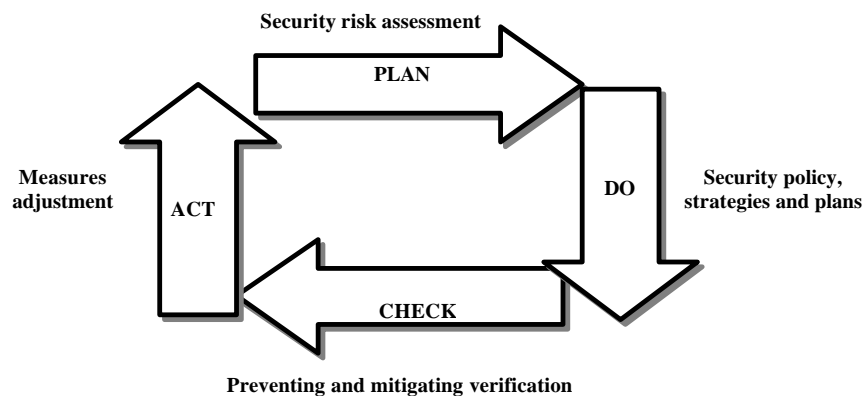


Figure 1: The Continuous Security Improvement (CSI) cycle

This is based on the fact that security threats are not static, and therefore all necessary activities prepared to cope with them should also be dynamic. The CSI

cycle begins with the planning, in which security threats are identified and their criticality and likelihood are determined, vulnerability is assessed and priority is assigned. The next stage is to develop, evaluate, and implement security policy, strategies, and plans to prevent and mitigate the effects of security breaches. As some security breaches may occur, the next step is to verify whether policy, strategies and plans implemented have successfully prevented or mitigated the impacts of successful security incidents, as well as collect additional information from these incidents for further adjustment in the security risk assessment. The next stage of the cycle is to take action, meaning that proper adjustments are conducted so as to complete the security management cycle. From this moment, a new management cycle is taking place, taking into consideration all new inputs from the previous steps. The cycle will thus continue and become more and more finely-tuned for better security management. The CSI cycle is illustrated in the following figure.

2.2 Risk-based security management and its connection with Business Continuity Management (BCM)

There is an interrelationship between risk management and BCM. Since security risk is a component of the organisation's risk portfolio, it is argued that the management of security should be based on sound risk management, and business continuity should also be one of the expected outcomes of security management. Indeed, the literature review has suggested that security management must be based on risk management in order to be effective, and the steps of the risk management process can be applied to address security risks. Broder [4] emphasises the benefits of risk-based security management, especially highlighting areas where greater (or lesser) security is needed through security risk identification, analysis and evaluation. ESPO [5] emphasises that a stable and reliable port brings risks under control, and believes that policies aimed at fighting terrorism should be clearly linked with other and existing initiatives aimed at fighting organised crime, piracy, fraud, smuggling and illegal immigration. Any measures and policies should furthermore be based on a serious assessment of the actual risks involved.

The steps of the risk management process have been woven into the security management process, in which security risks need to be identified, analysed and evaluated in order to provide the grounding for risk control strategies. Furthermore, the organisation also needs to develop a contingency plan as part of the process to help the organisation return its resilience, and this is clearly the expected outcome of security management in connection with BCM. The application of risk management in security risk management has been emphasised by many scholars and practitioners, especially the risk assessment to provide the background for risk control. A detailed study of vulnerability, criticality (consequence) and threat is necessary to formulate a security risk profile. It is argued that such a security risk assessment is the key to making IMO's ISPS Code effective. A risk-based security management process should also consist of four core elements: threat identification, risk assessment, acceptance criteria, and the implementation process of risk control. These are clearly the necessary steps of the risk management process so as to effectively manage security risks in transportation and maritime transport. Specifically, Iarossi [6] and Nolan [7] argue that an effective risk based security management process must take a holistic approach. There are three phases that must be considered within such an integrated process. First, it is necessary to

identify all possible threat scenarios. Then the risk of each scenario must be characterised (the threat of each scenario must be assessed, the vulnerability must be analysed, the possible consequences of each scenario must be determined). Finally, the information gained from this security risk assessment must be used to adjust the planned risk management controls that are already in place or that should be developed to address normal operation risks. A prioritised, risk-based approach to security management is a critical element in determining practical and affordable solutions. Once the risks are identified, assessed, and prioritised, action plans can be developed to mitigate the risks.

In short, it can be seen that the management of security, as an element of the organisation's risk portfolio, should be based on a sound risk management approach and be closely related to BCM in order to be effective. In this regard, security management should adopt and integrate the fundamentals of RM into its management process. Security threats, vulnerability and criticality must be examined and the security acceptance level must be set so as to provide a firm background for the implementation of any security optimisation strategy. The organisation, in conducting these management processes, should also communicate and consult with its internal and external stakeholders. Moreover, these processes need to be continuously monitored and reviewed so as to provide new inputs to keep security management abreast of changing security threats and their probability of occurrence, and therefore, be valid and effective. In addition, the organisation should also address business continuity management as an integral part of its security management, and have in place the necessary processes and procedures so that it can return to resilience once a security breach is successful. With all of these in mind, one can argue that the RM approach to security management and consideration of its relationship with BCM would be powerful management weapons for the organisation in the quest of achieving its goals and objectives.

3 Identification of CSFs of effective security management

Security management is effective only when it helps the organisation to achieve its goals and objectives by facilitating efficient business operations while protecting the organisation's resources from security threats. In this connection, it has been argued that the QM and RM approaches to security management (SM) can contribute valuable inputs. QM philosophies and principles are now adopted in not only SM but also RM and BCM, while both RM and BCM not only have an interrelationship with each other but also affect the good/effective SM. Today, many organisations are adopting a risk-based approach to security, and the move to a risk-based paradigm is a catalyst for moving security from a technical specialty to an organisational competency. Moreover, since modern organisations must continually adapt to their environment and emerging risks – risks that perhaps unknown until the organisation is impacted by them, it is critical that the organisation view security in the context of the larger picture – security as one of organisational or enterprise resilience. A resilience approach transforms the basic premise of security – that of 'locking down' an asset so that it is free from harm or attack – to one that positions security as a contributor to strengthening the organisation's ability to adapt to new risk environments and accomplish its missions. The three approaches of QM, RM and BCM to security management as discussed above lead to the following proposed critical success factors (CSFs) for

the effective management of security in any organisation, including maritime transport service providers as summarised in table 1 below:

Table 1: CSFs of effective security management

No.	Critical success factor	Code
01	Well-defined and clear security accountability and responsibility at all levels of the organisation	CSF1
02	Documented security processes and procedures	CSF2
03	Security threats, critical resources to be secured and impacts of security threats identified, analysed and evaluated	CSF3
04	Minimum security requirements for resources identified and risk acceptance level established	CSF4
05	Security risk levels clearly defined	CSF5
06	Security risk mitigation strategies and plans in place and clearly understood by operators	CSF6
07	Resource allocation plan to mitigate security risks based on defined security risk levels	CSF7
08	Contributions of employees, business partners and related agencies to security policy, strategies, and plans, including their changes if any, taken as essential inputs	CSF8
09	Emphasis on monitoring and reviewing all security processes and procedures, at all organisational levels	CSF9
10	Continuous review and improvement of security policy, strategies, plans, processes and procedures	CSF10
11	Use of specific organisational structures (security improvement committee, work teams, etc) to support security improvement	CSF11
12	Long-term benefits of security recognised by senior management executives	CSF12
13	Security policy, strategies and plans actively directed by senior management executives	CSF13
14	Allocation of adequate resources to security improvement efforts, including training	CSF14
15	Preparedness of the senior management executives to remove the root causes of security problems	CSF15
16	Employees encouraged to find and provide feedback on security problems	CSF16
17	Employee involvement in the design and planning of the security policy, strategies and plans	CSF17
18	Security training viewed as a long-term investment and service quality improvement facilitator	CSF18
19	Security policy, strategies and plans integrated in overall business policy, strategies and plans	CSF19
20	Security processes and procedures integrated in daily operation processes and procedures	CSF20
21	Technology-based solutions to security problems understood by senior management as not the only answer	CSF21
22	Security of information viewed as important as security of physical resources (assets, people, etc)	CSF22
23	Availability of detailed contingency plans to follow in the event of security breaches or incidents, continuously reviewed and updated	CSF23
24	Availability of detailed recovery plans to maintain business resilience after security breaches or incidents	CSF24

4 Empirical validation of CSFs

4.1 Research methodology

In order to empirically validate the 24 CSFs as identified previously a survey instrument was developed. This instrument was developed on the basis of an

exhaustive review of the literature and the subsequent research model. It has been refined several times based on the pilot study findings and on the comments and suggestions of the experts in the field. The instrument has been so developed in order to maximally capture all the CSFs of effective security management. The questionnaire begins with the guidelines in which the concept of effective security management is carefully explained, and the confidentiality of respondents is assured. The questions with respect to the various CSFs were jumbled and arranged in a random order in the instrument so as to avoid order bias. The respondents were asked to indicate their perception of the importance of each critical success factor of ESM on a five-point scale (from 1 indicating not at all important to 5 indicating very important). Since the unit of analysis is the maritime transport service providing organisations, the target population in this research is, therefore, encompassing the groups of shipping companies, port operators and freight forwarders/NVOCCs which are providing maritime transport services in Vietnam. 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*. This publication is a well-known and prestigious source of specialised information on maritime transport and the logistics business in Vietnam, and recognised by both professionals and governmental officials in the field. A list of 197 maritime transport service providing organisations from the directory in this publication, including 66 shipping companies, 49 port operators and 82 freight forwarders/NVOCCs, was used as the mailing list for this research. By the cut-off date, there were 119 returned questionnaires, including 42 from shipping companies, 43 from port operators, and 34 from freight forwarders. This represents a 60% response rate. The high response rate is due to the personal contact approach used followed by periodic follow-ups over telephone and also personal visits.

The following hypothesis was subsequently formulated:

The CSFs of effective security management in maritime transport are the 24 identified items stated above.

4.2 Analysis of findings

In order to test the hypothesis and validate the research CSFs, a number of statistical analyses have been conducted using the SPSS version 11.0 software. The descriptive statistics provide an overview concerning the variables (here are the critical success factors) in the survey. In this respect, the mean and standard deviation of each variable are calculated to see whether the variable could be accepted by the respondents and exist as a critical success factor in question. Based on the mean scores of all variables, a ranking order is established accordingly to reveal the magnitude of importance of each factor. Table 2 illustrates these descriptive statistics.

The standard deviation in response to each CSF is seen as quite small. It is seen that all the CSFs of the effective security management proposed are accepted by the respondents, in which CSF17 (Employee involvement in design and planning of security policy, strategies and plans) with the lowest mean score of 3.34 is still above the measurement scale with 3 being neutral. The most important CSF is CSF23 (availability of detailed contingency plans to follow in the event of security

breaches or incidents, continuously reviewed and updated), followed by CSF2 (documented security processes and procedures), and CSF24 (availability of detailed recovery plans to maintain business resilience after security breaches or incidents). Among these three most important critical success factors, two (CSF23 and CSF24) are related to incident handling and response within the scope of business continuity management. Moreover, it is emphasised that these factors are closely connected to quality management, as the contingency and recovery plans should be continuously reviewed and updated.

Table 2: Perceived importance of critical success factors

Critical success factor	Mean	Std. Deviation	Rank	Critical success factor	Mean	Std. Deviation	Rank
CSF23	4.66	0.56	1	CSF6	4.15	0.48	13
CSF2	4.58	0.57	2	CSF19	4.15	0.73	14
CSF24	4.56	0.62	3	CSF8	4.13	0.50	15
CSF5	4.44	0.58	4	CSF22	4.02	0.64	16
CSF14	4.42	0.54	5	CSF15	4.02	0.68	17
CSF1	4.42	0.60	6	CSF16	3.99	0.56	18
CSF13	4.39	0.55	7	CSF10	3.87	0.62	19
CSF7	4.34	0.57	8	CSF9	3.85	0.63	20
CSF4	4.28	0.52	9	CSF21	3.73	0.65	21
CSF3	4.25	0.52	10	CSF18	3.64	0.62	22
CSF12	4.21	0.68	11	CSF11	3.52	0.57	23
CSF20	4.16	0.74	12	CSF17	3.34	0.78	24

The respondents also highly rated documented security processes and procedures, and well-defined and clear security accountability and responsibility at all levels of the organisation (CSF1 and CSF2) are ranked as the second and sixth most important factors. Factors related to security risk assessment and risk-based security mitigation strategies and plans are also perceived among the most important critical success factors of effective security management in this survey. Specifically, respondents view the security risk levels clearly defined (CSF5) as the fourth most important factor, while other factors involving risk management (CSF3, CSF4, CSF6, CSF7) are also ranked as the eighth, ninth, tenth and thirteenth most important factors. It is noted that respondents view these as critically important ones since security risks should be clearly identified, analysed and assessed and these assessment should be the foundation upon which strategies and plans are based.

Factors related to the senior management's commitment and leadership are also highly appreciated by the respondents in that CSF14 and CSF13 are ranked as the fifth and seventh most important factors. It can be seen that effective security management requires not only the involvement and leadership of the senior management, but more importantly, that they should provide adequate resources for security improvement, including training as well. As anticipated, factors related to security design and process control (CSF20 and CSF19) are also highly ranked by the respondents being the twelfth and fourteenth most important critical success factors with mean scores of 4.16 and 4.15 respectively. In this respect, it is confirmed through the survey that effective security management is attributed by the security policy, strategies, plans, processes and procedures integrated in the overall business ones and should not be designed separately from the overall picture of business operations. Other factors involving communication and consultation with stakeholders, holistic approach and employee empowerment (CSF8, CSF22 and CSF16) also received relatively high ranking as critical success factors of effective security management. The survey also reveals that the quality principle of continuous improvement is recommended in security management, in

that security policy, strategies, plans, processes and procedures should be continuously reviewed and improved. This factor received a mean score of 3.87 and was ranked in nineteenth place. The least important CSF, as ranked by the respondents, was CSF17, employee involvement in design and planning of security policy, strategies and plans, although its mean score was still higher than the average consensus level in the scale. This magnitude of importance may be explained as, although employees should be encouraged to find and provide feedback on security problems (CSF16), the designs and planning of security policy, strategies and plans require the expertise and skills of specialised staff so that not all normal employees can be qualified and involved. Nevertheless, it can be seen from table 3 above that all these 24 CSFs are essential so that security in maritime transport can be effectively managed. In short, the hypothesis has been empirically tested and the critical success factors of effective security management have also been validated.

5 Conclusion

In summary, the proposed hypothesis has been empirically tested. The statistical analysis conducted in the survey has proved that this hypothesis is accepted in the context of Vietnamese maritime transport service providers. All 24 proposed factors are accepted as CSFs of effective security management in maritime transport with the lowest mean score of 3.34, which is above the average score of the scale. These CSFs are derived from the QM, RM and BCM approaches to security management. Among the most important factors, ones related to incident handling and response (CSF23 and CSF24) are perceived as the most and the third important factors, and have higher rankings than those involving security risk assessment and risk-based security mitigation strategies and plans (CSF3, CSF4, CSF5, CSF6 and CSF7). This finding more or less indicates that Vietnamese maritime transport service providers currently focus on 'situational' and short-term factors. Among the identified CSFs, the five most important ones are the following:

- Availability of detailed contingency plans to follow in the event of security breaches or incidents, continuously reviewed and updated (mean 4.66)
- Documented security processes and procedures (mean 4.58)
- Availability of detailed recovery plans to maintain business resilience after security breaches or incidents (mean 4.56)
- Security risk levels clearly defined (mean 4.44)
- Allocation of adequate resources to security improvement efforts, including training (mean 4.42)

In short, it has been empirically tested that all proposed 24 CSFs are valid and should be used as critical factors for success in effectively managing security in maritime transport, so as to satisfy security requirements while enhancing other business objectives. The confirmed implication of this research is that effective security management can be achieved by employing critical success factors derived from the fundamental principles of quality, risk and business continuity management. This research can also be extended by being conducted in various other social contexts in order to maximise its generalisability.

References

- [1] Lee, H. L. and Whang, S., Higher supply chain security with lower cost: lessons from Total Quality Management, <http://gobi.stanford.edu/ResearchPapers/Library/RP1824.pdf>, 2003.
- [2] Doak, R., Security measures & growing quality logistics practices, *Logistics quarterly*, **9(1)**, <http://www.lq.ca/issues/spring2003/articles/article04.html>, 2003.
- [3] Deming, W. E., *Out of the crisis*, MIT Technology Center for Advanced Engineering Study: Cambridge, MA, 1986.
- [4] Broder, J. F., *Risk analysis and the security survey*, Butterworth Publishers: USA, 1984.
- [5] ESPO, Port and maritime security, www.espo.be/policy/initialviewsFINAL.pdf, 2002.
- [6] Iarossi, F. J., Creating a safe and secure environment for the marine transportation of energy, <http://www.absconsulting.com/news/fji-nov182002.html>, 2002.
- [7] Nolan, T. M., Security and safety: real responses to maritime security threats, www.socp.org/archive/3-5-03/presentation-3-5-03/tn_abs.ppt, 2003.