航 運 季 刊
第十八卷 第二期
民國九十八年六月
頁 69 ～ 頁 87

Maritime Quarterly
Vol. 18 No. 2
June 2009
pp. 69~87

The Analysis of Probability and Impact and Relative Priority Evaluation of Information Systems Risk Factor in Maritime and Port Enterprise[1]

Myung-Hee Chang[2]

ABSTRACT

The purpose of this study is to manage the risk factor which can happen in running the information system of marine and port corporations and derive the suitable information system framework by analyzing and assessing the risk factor of information system among the corporations. The probability and impact analyses is constructed and also according to the analytical frame work of information system risk factor, the model for AHP analyses is constructed, and a survey is conducted subject to marine and port information system expert's. By analyzing the survey with AHP, the degree of the relative importance about the information system risk of the marine and port corporation is analysed. We found that marine and port information system expert's thought high level about probability and impact of information risk. Summarizes of the AHP result is as follows; First, it shows that the programing and the development error and the data input error are considered the most important factors by expert's of information system.

Keywords: risk factors of information system, probability, impact, framework of information system risk management in maritime and port, AHP

Ⅰ. Introduction

The rapid transfer to the world economy has been triggered by IMF relief loan in the late 1990s. As a result, the business environment surrounding enterprise is becoming more and more uncertain, and many risks are associated with one another. Therefore, the priority of risk management is further highlighted by the need for systematic management. There is a worldwide trend that government and regulatory agencies strengthen the corporations risk management standards to measure the level of risk and to require its mandatory disclosure. In particular, as changes in the external environment and internal IT(Information System) management risk grow, IT(Information System) business risk has been increased by the increasing IT(Information System) costs.

Information system risk means that unexpected operation snags of information system part encountered by intention or by accident are likely to affect the overall business operation of an

[1] This paper was published in the Journal of Shipping and Logistics, Vol. 25, no. 1, March, 2009, by the Korean Association of Shipping and Logistics Inc.

[2] Professor of Korea Maritime University, email : cmhee2004@hhu.ac.kr

corporations. According to the report, `IT risk management spread and technical evolution', published by Korea Software Industry Promotion Agency (2008), the risk occurrence of information system parts can lead to fatal results in business such as company revenue reduction, negative image spread, customer breakaway, and so on. It has also reported that the majority of the enterprise barely run the risk management of information systems, and even enterprise risk management, IT service management, and IT governance does not run the risk management focused on IT sectors properly.

Maritime and port industries has constructed and operated individual or integrated logistics information system networks with each distribution industry body or government ministries and offices in order to run the overall administration of physical distribution efficiently. Despite the priority of information system risk management, the logistics information systems are not prepared for various risks associated with information systems since the logistics information systems are primarily interested in distribution cost reduction, information sharing and productivity improvement. When information system risk occurs, most companies in the past rely on a backup system or their own experience and intuition to handle the risk, and it is hard to find the cases of the systematical risk management and treatment.

The risk management means occurrence probability management. Therefore, it does not guarantee that the risks will occur and inflict fatal damages on enterprises; however, it indicates that a fatal and irreversible loss will be actualized once the risk occurs. Several potential risks in enterprises include, accidents such as fires, terror threats, explosions, wars, strikes, civil disturbances, sabotages, paralyses of public facilities, building collapses, floods, heavy snowfalls, earthquakes, and earthquake tidal waves. When these risks occur, the following elements of enterprise survival are crucial: how to respond, how to minimize damage, how quickly return to normal business. Therefore, the risk management in modern enterprises means the enterprise survival strategy and the essential element of corporate management because immature risk management shortens the life of the enterprise.

In domestic case, the government agencies and the financial institutions as dominated forces have recognized the importance of information system risk management and built enterprise risk analysis models and disaster recovery systems actively. On the other hand, interest in the risk associated with information systems is still stuck at a relatively low level in the field of maritime and ports.

Therefore, the purpose of this study is to derive a risk factor evaluation model of maritime and port enterprises based on domestic and international preceding research and analysis methods of information system risks so that it suggests a proper management method of information system risk factor. In doing so, work experts of the maritime and port enterprise information system were participated in the analysis, and they analyzed information risk factor probability, impact, and relative priority.

Ⅱ. Theoretical Background and Preceding Studies

1. Definition and Types of Information System Risks

The definition of risk varies in different scholars, but all the definitions can be integrated

into the term 'uncertainty' in the psychological form caused by unpredictable phenomena in future.

Information system risk means a probability that unexpected operation snags of information system are likely to affect the overall operation of an enterprise. For example, Comair, a subsidiary of the U.S. airline Delta Airlines, has experienced the operation halt of the overall flight crew scheduling system due to the operation suspension of the fatal IT system on Dec. 24, 2004.

The recent enterprise operating systems emphasize integration and service; therefore, these systems rely on information technology more and more. For enterprises not supporting smooth operations of information system, the probability of being in irrecoverable trouble, namely risk, gets higher.

Information system risk management is to maintain security countermeasure against measured/evaluated risk up to a certain level. In addition, the risk management means threat reduction from the organization, procedures, personnel management, administration, hardware and software, and so on.

In this study, various definitions for the information system risk has been gathered to define it as 'an uncertain situation which can occur in enterprise information system environments(business process / information technology)'. As dependence on information systems has grown, risk factors have been increased. Therefore, the interest in the risk management system has been increased to effectively cope with the increasing risk factors.

Risk management is a series of processes to derive implementation strategies and system security policies, which matches the security policies and purposes of an organization, from the evaluation of information system risks and comparison of the costs and effects based on the evaluation result. Therefore, the preliminary consideration of risks in design steps of the organizational information system for each business field can result in its effect. According to the organizational environment and capacity, it has the advantage of support to operate countermeasures.

2. Preceding Studies on Information System Risk Factors

The classification purpose of information system risks is to check the enterprise means of risk analysis and to cope with the risks by grasping mutual relevance of the risk factors and promoting understanding of them.. Since domestic maritime and port enterprises have a low awareness of the information system risk and related researches are insufficient, information system risk factors have been extracted on the basis of the preceding studies targeting general companies to find the primary risk factors. The following is a summary of related studies. Most preceding studies of the information system risk are the researches on risk management of information system development projects.

Schmidt et al.(2001) suggested a checklist of risk factors in terms of project management of information system projects to which applies the latest technologies for the project managers of 3 countries such as the Finland, Hong Kong, the United States.

In the probabilistic simulation study of risk factors on software development risk management, Houston(2001) suggests a checklist of 30 risk factors for the risk areas without

categorization.

In the study of Business Continuity Management in preparation for information system disaster, JongGi Kim(2001) and others review a new concept of contingency planning suitable for the changing business environments and discuss the establishment methodology of emergency plans from the viewpoint of business continuity management in order to ensure the continuity of business activities. According to them, the risk assessment is carried on the basis of risk analysis for the information system risk assessment if the specific collection of data regarding a threat is possible after first evaluating the vulnerability by business influence analysis. It is necessary to measure risks for the evaluation of the risk level so that the expectation loss, which is measured by the multiplication of the threat probability and the loss size, is calculated by a proper risk analysis method selected as the process of asset loss analysis.

In the information system development projects, ChulYoung Chung, and DongKi Sohn(2006) review procedures and methods for managing risks and derive risk factors affecting its failure. In addition, each risk factor is evaluated to increase the understanding of risk factors and priorities are suggested for the project management. For the differentiation from the existing researches, the impacts on duration, cost, and quality are evaluated respectively, and the weight depending on the relative priority of risk factors is applied. With this case, they assert that the risk factors of information system projects do not affect only a specific part but also include their mutual association. In addition, they insist that the risk level for each risk factor be checked and that researches on the proposed risk factors and classification system be continued to consider countermeasures against each risk in the future.

In the actual-proof study regarding risk factors of information system projects, SukJin Cho(2006) and others suggest the information system project risk factors to practitioners in the domestic information system projects with the statistical objectivity. In risk analysis of the administrative information sharing system, Eunkyung Lee (2006) makes an actual-proof analysis based on the vulnerability guideline of IT systems provided by the Canada government and classifies risk factors derived from cause & result correlation analysis into a physical, infrastructure, technical, human, and procedural risk factor. As a result of cause and effect analysis per risk factor, each risk factor brings about a crisis because it raises an infringement of confidentiality, integrity, and availability. In particular, given the characteristics of public service, other important evaluation items, reputation/reliability degradation, are shown in addition to these three factors.

In the TaeDal Kim and HyongWon Lee(2007)'s study, they are interested in a series of risk management process automation of corporate IT risk management(Asset Identification, risk analysis, control design, control implementation, risk monitoring, risk response, risk assessment, control redesign and improvement). In the study, the characteristics of the information system risk management process are researched and analyzed intensively depending upon the research and development result of the Information Technology Risk Management System(ITRMS) in the domestic company, MetaRisk(Co.), and the cases of developed countries.

Ⅲ. Classification Scheme and Analysis Structure of Maritime and Port Enterprise Information System Risk Factors

1. Classification Scheme of Information System Risk Factors

In order to find common and standardized evaluation factors and criteria for the risk factors of maritime and port information system, this study considers the priority and the weight of risk factors suggested by each researcher, and it derives risk factors from the comparison and addition of risk factors suggested by institutions such as Canada, NFPA, TTA(Telecommunications Technology Association, 2000) on the basis of factors which present in the risk factor report proposed by the major information system risk management institution, the USA NIST. As a result, the first 72 risk factors can be found. In order to ensure the more accurate objectivity of the derived risks, 21 factors are finally confirmed through the consultation of the academic world and the research world(3 people), maritime and port company's computer experts(3 people), and so on. In Table 2, the classification scheme for the information system risk factors of maritime and port enterprises is drawn up. As shown in Table 2, information system risks of the maritime and port enterprise can be resulted from factors such as the errors and omission, fraud and theft, employee interfering operations, lack of supporting physical infrastructure, malicious hackers and industrial espionage, and malicious code. Each risk group is made up of its detailed factors.

Table 1 Examples of Categorical Causes and Potential Impact of Information System Risk

Category	Definition	Causes	Potential Impacts
security	risks caused by illegal access manipulation, and use of information	-external attacks -malicious Code -physical destruction -unauthorized access -dissatisfied employees -Too many different platforms and messaging Types	-information damage -outsider frauds -Identity theft -robbery of financial assets -decrease of corporate reputation and brand image - property damage
availability	risks caused by blocking of business process, or data access	-hardware problems -network problems -deficiency of change management process -data center problems -uncontrollable problems	-business transactions cancellation and sales opportunity loss -decrease of trust from customers, partners, employees, -interruption/delay of business-critical process
performance	risks caused by access delay to business processes or data	-invalid system architecture -network contention -inefficient code -lack of capacity	-decrease of customer satisfaction -decrease of Customer / Partner Loyalty -user productivity decrease -productivity decrease of information technology
compliance	risks caused by violation of laws, regulations, or IT policy compliance items	-each regional laws -legal action -Internal information technology handling for compliance support -inappropriate external compliance standards	-decrease of corporate reputation -The leakage of confidential customer information, -lawsuits -the productivity of corporate executives

Source : Semantic Korea (2007), “Semantic IT Risk Management Report Issue #1"

Table 2　the classification scheme for the information system risk factor

Risk Classification	Risk Factors
errors and omission	・all types of data entry errors and omission ・programming and development errors ・installation and maintenance errors
fraud and theft	・fraud and theft for equipment and facilities (including general user, IT technician, predecessors, outsiders) ・data manipulation and theft (including general user, IT technician, predecessors, outsiders)
employee interfering operations	・destruction of hardware or facilities ・implantation of the logical bomb damaging program or a data ・data deletion and change ・criminal activities with the hostage of data ・strike
lack of physical infrastructure support	・power supply trouble ・communication line trouble ・natural disasters such as fire, flood, weather ・terrorist activities
malicious hackers and industrial espionage	・hacker intrusions ・industrial espionage ・espionage of foreign intelligence agencies
malicious code	・virus infiltration ・infiltration of worms ・infiltration of trojan horses ・threats to personal and confidential affairs

2. Analysis Methods for Information System Risk Factors

1) Risk factor analysis methods

In the past, 1~2 methods for risk factor analysis were bused to measure the risk. However, according to recent TTA (Telecommunications Technology Association, 2000), various methods are recently combined from at least one or two ways to more than a dozen different ways during the risk process in order to perform risk analysis.

According to SinWon Kim(2001), the risk analysis methods can be divided into two methods: quantitative analysis and qualitative analysis.　In Table 3, the qualitative approach is compared the quantitative approach for the risk analysis approach.

Table 3 the qualitative approach and the quantitative approach for the risk analysis approach.

Category	Quantitative Approach	Qualitative Approach
concept	value analysis of expected risk =risk probability × risk size	Difficult to express the size of the loss in currency value. The risk size is expressed in a technical variable.
types	mathematical formula access method, probability distribution deduction method, probability control, Monte Carlo simulation and legacy data access method	methods according to Delphi, scenario, ranking, fuzzy matrix, questionnaire, AHP
major use areas	USA	Europe
scale	annual loss expectancy(ALE)	scoring method(5 point scale, 10 point scale)
advantages	cost / value analysis, budget planning, data analysis are easy	Possible to evaluate information difficult to convert it into an amount of money. Analysis time is short. Easy to understand
disadvantages	analysis time, effort, and cost are high	Evaluation result is subjective and varies depend on people
tools	BDSS, RISKCALK, RANK-IT, RISKWATCH, AnalyZ, LRAM	CRAMM, LAVA, RISKPAC, MARION, NetRISK

Source : Sin-Won Kim(2001), pp. 6-8

Until now, most researches have used subjective probability values to express the qualitative risk factors in quantitative numbers. In this study, first, since a number of information system risk factors should be analyzed at the same time, probability analysis is performed on the probability and impact of risk factors. Next, for the evaluation regarding the information system risk factors, Saaty's AHP technique is used to determine the weight reflecting the relative priority.

2) AHP concept and structure configuration for evaluation of the relative priority

AHP is a multiple criteria decision-making technique which supports multifaceted criteria for evaluation and the decision made by multiple decision makers. AHP is characterized by a comprehensive framework for the problem resolution which considers both quantitative and qualitative factors at the same time on the basis of the consistent judgment made by the evaluator via the pair-wise comparison, not via the absolute evaluation regarding a criterion. The following four steps of the AHP evaluation techniques will be performed in the operation. First, the decision-making problems are divided into layers of interrelated decision-making items to set the decision hierarchy. Second, the pair-wise comparison of the decision factors is performed to collect data. For the pair-wise comparison is applied to measure the rate of 9 points. Third, the fixed value method is used to estimate the relative weights of the decision-making factors. In particular, a big advantage of the AHP evaluation technique is

discussed with the consistent index of the replies which can be generated in the process of estimation. Fourth, the relative weights of the decision-making factors are synthesized to get a comprehensive ranking of various alternatives which becomes the evaluation objects.

In this study, risk factors of maritime and port information systems get categorized and hierarchical for the purpose of the systematical identification and management of risk factors. For this reason, Saaty's AHP technique is applied to the risk factor evaluation model.

In order to ensure the more accurate objectivity of the risks derived by group, 21 factors are finally confirmed through the consultation of the academic world and the research world(3 people), maritime and port company's computer experts(3 people),and so on. As shown in Table 2, the classification scheme for the information system risk factors of maritime and port enterprises is drawn up and the hierarchy of this risk factor classification scheme can be represented as shown in Figure 1.

In this study, the form of the AHP hierarchy configuration is divided into three steps. Therefore, in the first step, information system risk factors are determined by the evaluation criteria. The second step includes the errors and omission, fraud and theft, employee interfering operations, lack of physical infrastructure support, malicious hackers, and industrial espionage as the elements affecting the information system risk factors which indicate the goal of the first step are included. In the third step, the detailed elements of the second step factors are included.

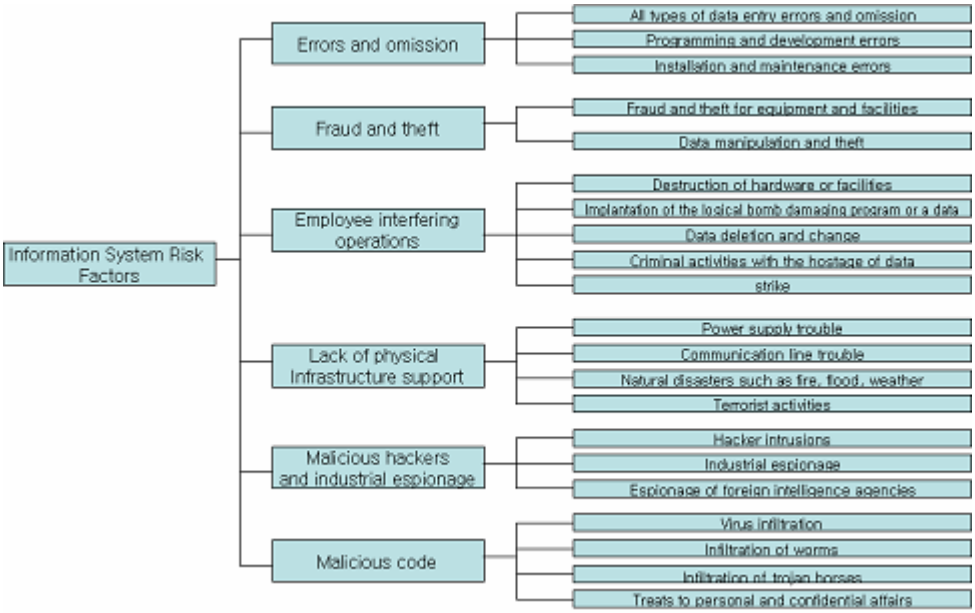


Figure 1 The AHP Hierarchy to Evaluate the Information System Risk Factors of Maritime and Port Enterprises

Ⅳ. The Probability and Impact Analysis and the Relative Priority Analysis for the Information System Risk Factors in Maritime and Port Enterprises

1. Survey Configuration and Sample Objects

This study consists of 2 different types of questionnaires.

First, if an ordinal method is used to obtain the probability and impact of information system risk factors, the survey is configured to extract the linear value(0.1/0.3/0.5/0.7/0.9) which is typically used.

The second survey used the 9-point scale proposed by Saaty in order to evaluate the relative priority of information system risk factors and presents the explanation of each variable. The Survey has been held from May 10, 2008 to May 20, 2008, and for the survey data collection, the questionnaire is collected via the e-mail or visit, after the study purpose is explained to the assigned person in the survey target company over the phone. It is important for AHP to analyze with the opinions of experts rather than the quantity of the survey in order to meet the purpose of the survey; therefore, the survey targets are limited to the experts in the information system-related fields of the maritime and port sector. KieSung Oh has surveyed 10 web site experts by using the AHP to select the best web sites. YangCheo Jang and ByeongSeok Ahn have considered the opinions of 7 experts to select a information system development company by applying the AHP analysis. Tam and Tummala have used the answers from 5 experts to select a telecommunication company by applying the AHP analysis. Therefore, in this study, the survey targets the major information system-related experts(position: manager or above, technical level: advanced technicians or more, working years: 7 years or more) rather than the number of the respondents. Table 4 shows the survey target companies and the reply results.

The Expert Chose program is used to apply the reply results, which obtained from the experts via a survey, to AHP model.

Table 4 Survey Target Companies and the Reply Results

survey target companies	company	quantity of distributed questionnaires	
	terminal management and operating company	5	12
	shipping company	3	
	total logistics company	4	
reply results (significant questionnaires)	terminal management and operating company	3	collect 10(83%) significant questionnaires : 5 (equal to or less than 0.1 by Consistency Ratio of Saaty)
	shipping company	1	
	total logistics company	1	

2. The Probability and Impact of the Information System Risk Factors in Maritime and Port Enterprises

1) Occurrence probability

The method using risk factor values is to determine the occurrence probability and impact. The occurrence probability means the probability of the corresponding risk factor.

The risk management means the management of the probability. Therefore, there is no guarantee that the risks will occur and inflict fatal damages on enterprises; however, a fatal and irreversible loss can be predicted once the risk occurs.

In this study, the probability of information system risk factors in maritime and port enterprises has been researched from 5 experts in the related fields, and the average and standard deviation of the probability values are shown in Table 5.

Table 5 The Probability of Information System Risk Factors in Maritime and Port Enterprises

Classification of IS Risk Factors	IS Risk Factors	Probability (means)	Standard Deviation	Rank
errors and omission	all types of data entry errors and omission	0.50	0.200	2
	programming and development errors	0.46	0.261	3
	installation and maintenance errors	0.38	0.228	6
fraud and theft	fraud and theft for equipment and facilities	0.1	0.000	11
	data manipulation and theft	0.1	0.000	11
employee interfering operations	destruction of hardware or facilities	0.18	0.179	9
	implantation of the logical bomb damaging program or a data	0.1	0.000	11
	data deletion and change	0.54	0.219	1
	criminal activities with the hostage of data	0.1	0.000	11
	strike	0.18	0.110	8
lack of physical infrastructure support	power supply trouble	0.38	0.179	5
	communication line trouble	0.38	0.110	4
	natural disasters such as fire, flood, weather	0.34	0.219	7
	terrorist activities	0.1	0.000	11
malicious hackers and industrial espionage	hacker intrusion	0.14	0.089	10
	industrial espionage	0.14	0.089	10
	espionage of foreign intelligence agencies	0.14	0.089	10
malicious code	virus infiltration	0.38	0.179	5
	infiltration of worms	0.34	0.219	7
	infiltration of trojan horses	0.34	0.219	7
	threats to personal and confidential affairs	0.18	0.110	8

As shown in Table 5, you can notice that information system experts of maritime and port enterprises judge 'the data deletion and change '(0.54) to be the first rank as the highest factor, 'data entry error and omission of all kinds of data'(0.50) to be the second rank, and 'programming and development error'(0.48) to be the third rank.

2) Impact on enterprises

The impact of information system risk factors means that unexpected operation snags of the information system part encountered by intention or by accident are likely to affect the overall business operation of an enterprise.

In this study, the impact of information system risk factors in maritime and port enterprises has been researched from 5 experts in the related fields, and the average and standard deviation of the impact values are shown in Table 6.

As shown in Table 6, you can recognize that information system experts of maritime and port enterprises judge 'destruction of hardware and facilities'(0.82) to be the highest factor of the impact on enterprises. The reason for showing such probability values can be explained with the following interpretation that destruction of hardware and facilities can cause more damages compared to other types of business because the maritime and port sector spends more money on facility investment. The next highest impact can be observed with the following factors such as 'data manipulation and theft'(0.78), 'implementation of a logical bomb to damage programs or data'(0.78), 'terrorist activities' (0.78), 'hacker intrusions' (0.78) factors and so on.

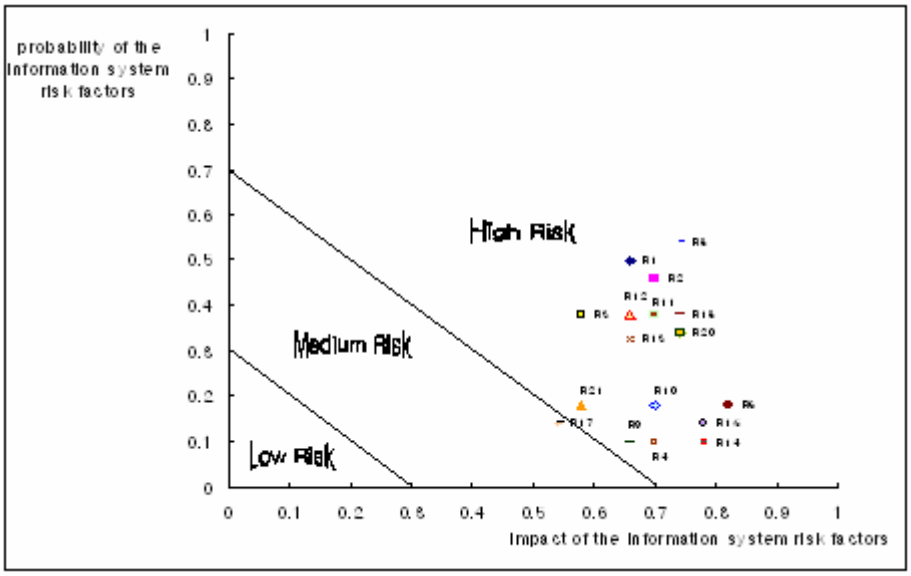
3) Risk factor rank

The Probability of occurrence and the probability of Impact are configured to the PI matrix and the Risk Degree can be expressed as the value generated from the multiplication of the probability(P) and the impact(I). According to DOE, this method can be used to quantify the risk results which revealed by a checklist, and so on. Typically, a PI value less than or equal to 0.3 is considered as the low-ranking risk, a PI value between 0.3 and 0.7 is considered as a middle-ranking risk, and PI values more than or equal to 0.7 is considered as a high-ranking risk which needs to be managed at the enterprise level.

The probability and impact of information system risk factors in maritime and port enterprises has been researched from 5 experts in the related fields, and the probability values are used to draw a graph of the risk ranks generated with the PI matrix as shown in Figure 2. As shown in Figure 2. you can notice that information system experts of maritime and port enterprises assess the risk probability and the risk impact on the enterprises as a high rank regarding information system risk factors.

Table 6 The Impact of Information System Risk Factors in Maritime and Port Enterprises

Classification of IS Risk Factors	IS Risk Factors	Impact (means)	Standard Deviation	Rank
errors and omission	all types of data entry errors and omission	0.66	0.167	7
	programming and development errors	0.7	0.167	4
	installation and maintenance errors	0.58	0.228	9
fraud and theft	fraud and theft for equipment and facilities	0.7	0.283	6
	data manipulation and theft	0.78	0.179	2
employee interfering operations	destruction of hardware or facilities	0.82	0.179	1
	implantation of the logical bomb damaging program or a data	0.78	0.179	2
	data deletion and change	0.74	0.167	3
	criminal activities with the hostage of data	0.66	0.219	8
	strike	0.7	0.200	5
lack of physical infrastructure support	power supply trouble	0.7	0.200	5
	communication line trouble	0.66	0.167	7
	natural disasters such as fire, flood, weather	0.66	0.167	7
	terrorist activities	0.78	0.179	2
malicious hackers and industrial espionage	hacker intrusion	0.78	0.179	2
	industrial espionage	0.54	0.261	10
	espionage of foreign intelligence agencies	0.54	0.261	10
malicious code	virus infiltration	0.74	0.167	3
	infiltration of worms	0.74	0.167	3
	infiltration of trojan horses	0.74	0.167	3
	threats to personal and confidential affairs	0.58	0.228	9



※ Risk5=Risk7=Risk14, Risk16=Risk17, Risk18=Risk20

Figure 2 Graph of the Risk Ranks Generated with the PI Matrix in Maritime and Port Enterprise

3. AHP Analysis Result Regarding Information System Risk Factors of Maritime and Port Enterprises

In Figure 2, the information system experts of maritime and port enterprises evaluate the information system risk factors, the risk probability and risk impact for companies, highly. when information system risks occur in a maritime and port company, the priority of the risks can be offered by analyzing the relative priority of these information system risk factors

AHP is capable of reviewing the reliability of the survey by calculating the Consistency Ratio(CR) to determine whether respondents have been consistent with the rating.

The Consistency Index divided by RI (Random Index) in order to obtain the Consistency Ratio. According to Saaty, the survey result of the respondents with the CR value equal to or less than 0.1 can be said with reasonable consistency. In this study, the theory of Saaty(1980) is applied, and the response with the layer Consistency Ratio equal to or less than 0.1 is considered to be reliable. Total responses of 5 volumes turn out to be reliable and these responses are used for the analysis of the model which evaluates risk factors of maritime and port information systems. The numerical integration method, which integrates the evaluation results of each individual by using a geometric mean after analyzing the results, is applied to the procedure of layer analysis process in order to calculate the relative priority of each factor and the integrated priority of each lower-part factor.

Regarding information system risk factors of maritime and port enterprises, the analysis of the relative priority of the first layer is shown in Table 7. As shown in Table 7, the relative priority is shown according to the following priority: the errors and omission(0.265), lack of supporting physical infrastructure(0.177), malicious hackers and industrial espionage(0.155),

malicious code(0.147), employee interfering operations(0.144), fraud and theft(0.111).

Table 7 The Analysis of the Relative Priority of the First Layer on Information System Risk Factors of Maritime and Port Enterprises

Information System Risk Factors (First Layer)	Relative Priority	Consistency Ratio
errors and omission	0.265	0.01
fraud and theft	0.111	
employee interfering operations	0.144	
lack of physical infrastructure support	0.177	
malicious hackers and industrial espionage	0.155	
malicious code	0.147	

Regarding information system risk factors of maritime and port enterprises, the analysis of the relative priority of the second layer is shown in Table 8.

Table 8 The Analysis of the Relative Priority of the Second Layer on Information System Risk Factors of Maritime and Port Enterprises

First Layer on Information System Risk Factors	Relative Priority	Second Layer on Information System Risk Factors	Consistency Ratio	Relative Priority
errors and omission	0.265	all types of data entry errors and omission	0.01	0.333
		programming and development errors		0.500
		installation and maintenance errors		0.168
fraud and theft	0.111	fraud and theft for equipment and facilities	0.00	0.333
		data manipulation and theft		0.667
employee interfering operations	0.144	destruction of hardware or facilities	0.00	0.260
		implantation of the logical bomb damaging program or a data		0.172
		data deletion and change		0.237
		criminal activities with the hostage of data		0.115
		strike		0.217
lack of physical infrastructure support	0.177	power supply trouble	0.01	0.358
		communication line trouble		0.300
		natural disasters such as fire, flood, weather		0.202
		terrorist activities		0.140
malicious hackers and industrial espionage	0.155	hacker intrusion	0.00	0.398
		industrial espionage		0.305
		espionage of foreign intelligence agencies		0.297
malicious code	0.147	virus infiltration	0.01	0.232
		infiltration of worms		0.292
		infiltration of trojan horses		0.268
		threats to personal and confidential affairs		0.208

Regarding information system risk factors of maritime and port enterprises, the relative priority of the second layer factors are reviewed as follows.

First, the analysis results of the second layer factors of the first layer errors and omission are shown according to the following priority: programming and development error(0.500), data entry error and omission of all kinds of data(0.333), and installation and maintenance errors(0.168).

Second, the analysis results of the second layer factors of the first layer fraud and theft are shown according to the following priority: data manipulation and theft (0.667), fraud and theft for equipment, and facilities(0.333).

Third, the analysis results of the second layer factors of the first layer employee interfering operations are shown according to the following priority: destruction of hardware of facilities(0.260), data deletion and change(0.237), strike(0.217), implantation of the logical bomb damaging program or a data(0.172), and criminal activities with the hostage of data(0.115).

Fourth, the analysis results of the second layer factors of the first layer lack of physical infrastructure support are shown according to the following priority: power supply trouble(0.358),communication line trouble(0.300), natural disasters such as fire, flood, weather(0.202), and terrorist activities(0.140).

Fifth, the analysis results of the second layer factors of the first layer malicious hackers and industrial espionage are shown according to the following priority: hacker intrusions(0.398), industrial espionage(0.305), and espionage of foreign intelligence agencies(0.168).

Finally, the analysis results of the second layer factors of the first layer malicious code are shown according to the following priority: infiltration of worms(0.292), infiltration of trojan horses(0.268), virus infiltration(0.232), and threat to personal and confidential affairs(0.208).

4. The Integrated Priority Analysis for the Information System Risk Factors of Maritime and Port Enterprises

The relative priority of each item is integrated to get a comprehensive ranking of each group whose factors are to be evaluated. In other words, on the basis of the priority of the second layer, the priority of sub-layers is multiplied in order to obtain the final priority of each group factors finally as shown Table 9.

According to the final priorities of the detailed factors regarding information system risk factors, the priority of programming and development errors (the 1st-layer factor: errors and missing factors) turns out to be 0.133 (0.265 * 0.500) and it indicates the highest relative priority among information system risk factors of maritime and port enterprises.

Rank	First Layer on Information System Risk Factors	Second Layer on Information System Risk Factors	Relative Priority
1	errors and omission	programming and development errors	0.133
2	errors and omission	all types of data entry errors and omission	0.088
3	fraud and theft	data manipulation and theft	0.074
4	malicious code	infiltration of trojan horses	0.063
5	employee interfering operations	destruction of hardware or facilities	0.062
6	errors and omission	installation and maintenance errors	0.053
7	lack of physical infrastructure support	natural disasters such as fire, flood, weather	0.047
8	malicious code	threats to personal and confidential affairs	0.046
9	malicious hackers and industrial espionage	hacker intrusion	0.045
10	lack of physical infrastructure support	terrorist activities	0.043
11	employee interfering operations	strike	0.039
12	malicious code	infiltration of worms	0.037
12	malicious hackers and industrial espionage	industrial espionage	0.037
13	employee interfering operations	data deletion and change	0.036
14	lack of physical infrastructure support	communication line trouble	0.034
14	employee interfering operations	implantation of the logical bomb damaging program or a dat	0.034
15	employee interfering operations	criminal activities with the hostage of data	0.031
15	malicious hackers and industrial espionage	espionage of foreign intelligence agencies	0.031
16	lack of physical infrastructure support	power supply trouble	0.025
16	fraud and theft	fraud and theft for equipment and facilities	0.025
17	malicious code	virus infiltration	0.017

Ⅴ. Conclusion

In this study, regarding information system risk factors in maritime and port enterprises, risk-ranking distribution is examined through the probability matrix of occurrence and impact, and the relative priorities of these risk factors is evaluated by using AHP as the experts in the related fields classify most risk factors as a high-ranking factor.

Regarding information system risk factors in maritime and port enterprises, 20 factors out of 21 are categorized as a high-ranking risk as the result of the investigation on the risk-ranking distribution through the probability matrix of occurrence and impact. From this result, you can notice that information system experts of maritime and port enterprises recognize the risk

probability and the high impact on the enterprises in case of actual risk occurrence. It is the fact that the maritime and port sector spends more money on facility investment and maritime and port-related services are automated on the basis of information technologies. Since the probability and the impact of information system are considered highly, the systematic management of information systems is required at the enterprise level. The information system risk management is able to effectively link business and information systems and to ensure reliability. Therefore, The maritime and port enterprises will be required to build IT governance actively in order to secure the business persistence and to cope with external regulation effectively.

Regarding information system risk factors in maritime and port enterprises, the analysis results of relative priorities which is generated by using AHP analysis are summarized as follows. First, the information system experts of maritime and port enterprises consider the risk factors, errors and omission(0.265), to be the most important. That is, since the respondents are information system experts who directly handle information systems, data, and programming, you can notice that they consider the following factors to be relatively important: programming and development errors(0.133) or data entry error and omission of all kinds of data(0.088), and so on. Second, the data manipulation and theft(0.074) of the fraud and theft factor is also considered to be important in comparison with other factors. Given the fact that the data manipulation and theft is perceived as a more important factor, the practical experts recognize information and knowledge resources more important than hardware, and the thorough management and security of the data resources will be required to overcome such risks. Third, the Trojan horse penetration factor (0.063) corresponding to a malicious code factor turn out to be more dangerous than general virus or worm infiltration. For this reason, maritime and port enterprises are very aware of the security management of information systems in a basic level, but they regard the Trojan Horse penetration, which does not show its symptoms and suddenly appear to cause fatal damages to the system, as a high risk. Therefore, it is necessary for maritime and port enterprises to manage the security risk which results from the illegal access, manipulation, and use to information.

Fourth, the destruction of hardware or facility factors(0.062) corresponding to the employee sabotage is described as an important factor because the maritime and port sector spends more money on facility investment. The strike of Port and Transport Workers Unions can also happen from time to time, and the 1st union sabotage targets on destroying hardware or facilities. In addition, natural disaster factors(0.047) such as fire, flood, and weather are considered as important information system risk factors of maritime and port enterprises. Since the maritime and port industry spends more money on facility investment, the natural disasters beyond control causes severe damages to enterprises. This case has been experienced with Typhoon Maemi. Therefore maritime and port sectors need to import (Enterprise Risk Management : ERM) in order to minimize the damages, which are caused by fire, flood, and weather, through the analysis of risk probability and impact. Busan Port Authority has already promoted the development and introduction of ERM from 2007.

The significance of this research is as follows. First, there is a probability that information system risk factors can bring fatal damage in maritime. port enterprises; however, the post-management level, which means the management after risk occurrence, still remains until

now. For this reason, information system risk factors are introduced and the necessity of systematic risk management is recognized with risk ranking distribution demonstrated through the analysis of probability and impact. Second, when information system risks of maritime and port enterprises occurs, the standards are proposed to consider the counterplan for risk factors according to the relative priority-ranking result of expert opinions. As a result, the damages in case of risk occurrence can be minimized. Third, the framework used for evaluating risk factors in maritime and port enterprises is practically suggested by applying information system risk factors to maritime and port enterprises.

This study has the significance of academic and practical implications, but there is a limit to generalize the results since the analysis is only done with the opinions of 5 information system experts in maritime and port enterprises. According to the characteristics of AHP, it cannot be said that surveys for many experts can increase the reliability of the results, but it is necessary to investigate with many more experts in order to generate more objective analysis of risk factors and to perform priority analysis.

References

1. Jung, C. Y. and Son, D. K., "An Exploratory Study for the Evaluation of Risk Factors in Information System Development Using AHP," ***The Journal of Information Systems***, Vol. 15, No. 2, pp. 77-93, 2006.
2. CSE, *Guide to Security Risk Management for IT Systems*, *Communications Security Establishment*, Government of Canada, 1998.
3. Kim, D. K. and Kwon, O. K., "A Study on the Development of Criteria and Priority Orders for Selecting Third Party Logistics Companies," ***Operations Research***, Vol. 20, No. 2, pp. 151-164, 2003.
4. Straub, D., "Effective IS Security: An Empirical Study," ***Information System Research***, Vol. 1, No. 3, pp. 255-276, 1990.
5. Houston, D. X., Mackulak, G. T. and Collofello, J. S., "Stochastic Simulation of Risk Factor Portentil Effects for Software Development Risk Management," ***The Journal of Systems and Software***, Vol. 59, pp. 247-257, 2001.
6. DOE, *Risk Analysis Management*, Good Practice Guide GPG-FM-007, p. 33, 1996.
7. Lee, E. K., "A Study on the Analysis of Information Risk for Risk Management," Dongguk University Master's Thesis, 2006.
8. Zahedi, F., "The Analytic Hierarchy Process-A Survey of the Method and Its Applications," ***Interfaces***, Vol. 16, No. 4, pp. 96-108, 1986.
9. Urban, G., Sultan, F. and Qualls, W., "Placing Trust at the Center of Your Internet Strategy," ***Sloan Management Review***, Fall, pp. 39-69, 2000.
10. Yang, H. D., "IT Risk Management, " ***Digital Times***, 2008.
11. Gillbert, A., "Risk Analysis: Concepts and Tools," ***Datapro Reports on Information Security***, pp. 102-112, 1991.
12. Kim, H., *Construction Planning and Decision*, Kimoongdang.
13. Kim, J. B., "A Study on the Port Risk Management," ***The Journal of Korean Association of Shipping***, No. 12, pp. 199-226, 1991.
14. Tregear, J., "Risk Assessment, " ***Information Security Technical Report***, Vol. 6, No. 3, pp.

19-27, 2001.
15. Kim, K., Park, J. S. and Kim, B. H., "A Risk Analysis Model for Information System Security," ***Journal of Korean Institute of OA***, Vol. 7, No. 3, pp. 60-67, 2002.
16. Oh, K. S., "A Study on Optimal Web Site Selection and Quality Evaluation, Using AHP," ***The KIPS Transactions : Part D***, Vol. 11-D, No. 2, pp. 381-386, 2004.
17. Cho, K. T., Cho, Y. T. and Kang, H. S., *AHP Decision of Leading Leader*, Donghyun, 2005.
18. Korea SW Industry Promotion Agency, "The Diffusion of IT Risk Management and Evolution of Technical," *SW Industrial Trend*, 2008.
19. Tam, M. C. Y. and Tummala, V. M. R., "An Application of AHP in Vendor Selection of Telecommunications Systems," ***Omega***, Vol. 19, No. 2, pp. 171-182, 2001.
20. NFPA, *Standard on Disaster/Emergency Management and Business Continuity Programs*, 2007.
21. NIST, *Risk Management Guide for Information Technology Systems Recommendations of the Institute of Standards and Technology, NIST SP* 800-30, 1998.
22. NIST, *Risk Management Guide for Information Technology Systems, Special Publication* 800-30, 2001.
23. Rainer, R., Snyder, C. and Carr, H., "Risk Analysis for Information Technology," ***Journal of Management Information System***, Vol. 8, No.1, pp. 129-147, 1991.
24. Schmidt, R., Lyytinen, K., Keil, M. and Cule, P., "Identifying Software Risk: An International Delphi Study," ***Journal of Management Information System,*** Vol. 17, No. 4, pp. 5-36, 2001.
25. Jarvenpaa, S., Tractinsky, N. and Vitale, M., "Consumer Trust in an Internet Store," ***Information Technology and Management***, Vol. 1, pp. 45-71, 2000.
26. Kim, S. W., "A Study of Information System Security Risk Analysis Model," Sogang University Master's Thesis, 2001.
27. Semantic Korea, "Semantic IT Risk Management Report Issue #1".
28. Kim, T. D. and Lee, H. W., "The Research Regarding an Information System Risk Management Process Characteristics," ***The KIPS Transactions : Part D***, Vol. 14-D, No. 3, pp. 303-310, 2007.
29. Saaty, T. L., "Modeling Unstructured Decision Problems-The Theory of Analytical Hierarchies," ***Mathematics and Computers in Simulation***, pp. 147-158, 1978.
30. Saaty, T. L., "How to Make a Decision: The Analytic Hierarchy Process," ***European Journal of Operational Research***, Vol. 48, No. 1, pp. 9-26, 1990.
31. Saaty, T. L., *The Analytic Hierarchy Process*, Mcgraw-Hill, 1990.
32. Telecommunications technology Association, Risk Analysis and Management Standards for Public Information Systems Security-Risk Analysis Methodology Model, 2000.
33. Duncan, W. R., *A Guide to the Project Management Body of Knowledge 2000 edition*, Project Management Institute, 2000.
34. Jang, Y. C. and Ahn, B. S., "A Study on the Selection of Information System Developer using AHP," ***Journal of Korea Society of IT Services***, Vol. 5, No. 3, pp. 187-200, 2006.