Information Security Workforce Planning in Korea

Hyo-Jung Jun, Tae-Sung Kim, Hee-Kyung Kong
Department of MIS, Chungbuk National University
12 Gaeshin-dong, Heungduk-gu, Cheongju, Chungbuk 361-763, Korea
phdhyo@naver.com, kimts@chnungbuk.ac.kr, konghk@paran.com

Keywords: information security workforce, causal-loop diagram, AHP

Summary: *The workforce suppliers have to qualify capabilities of workforce to meet the demand of industries. As training makes workforce qualified, the gap of workforce supply and demand can be controlled sufficiently. The fundamental purpose of this study is to describe that national information security workforce policies have to be set based on information technology trend to meet workforce demand, without causing supply surplus or shortage. With causal-loop diagram, we demonstrate framework of information security workforce market which is made by tangled relationships between suppliers and demanders. Then, with analytic hierarchy process, we make a study model which can describe how to set workforce policies based on the technology development trend.*

1. Introduction

Korea is positioning itself as a very promising country in informatizaion and has become a country with the world-class broadband employment ratio at the beginning of the 21st century. Since 2003, the Korean government, the ministry of information and communications, has executed 'Broadband IT Korea Vision 2007' to enhance transparency, efficiency, and the innovative delivery of information services (see Table 1).

As the society has entered into the information age, new types of societal problems, such as the leaking of personal information, misuse of the IT system, worldwide computer hacking via the Internet, and so on, have emerged. It was imperative to react to such threats properly at the national level, and integrated and systematic information security services were required. To make secure information society, the Korean government has deployed many policies and developed many number of technologies related to protection from attacks of the information threats.

As information threats diffuse, the information security industry becomes a major concern. The size of Korean information security industry already has gone up to 696.7 billion won in 2005 (NIS, 2005). It means that the size of industry has been entering stable growth stage and the emergent demand of industry is not expansion of the size but sufficient supply of workforce. But, the information security workforce of Korea is predicted that the gap of supply and demand will be 22 thousand people from 2003 to 2007 (MIC, 2002). For stable and continuing development of information security industry, the Korean government has implemented various policies to promote the information security workforce. Those policies have been successful to supply enough number of workforce, but not successful to supply workforce to meet the various requirements of the demand.

Table 1. Current status of informatization in Korea (Unit: in thousand, in billions won)

section	2001	2002	2003	2004
Households of broadband Internet	7,810	10,400	11,180	11,920
Subscribers of Internet	24,380	26,270	29,220	31,580
PC propagation	22,490	23,500	24,240	26,200
Subscribers of mobile lines	29,040	32,340	33,590	36,590
Users of internet banking	11,310	17,710	22,750	24,270
Size of e-commerce dealings	118,980	177,810	235,025	314,079

* The population of Korea is 47millions in 2005
** Source: NCA(2005). *2005 National Informatization Whitepaper.*

The main point of this study is that national workforce policies of information security industry have to be set based on information technology development trend to meet workforce demand sufficiently, without causing surplus or shortage of supply. With causal-loop diagram, we demonstrate framework of information security workforce market which is made by tangled relationships between many suppliers and demanders. Then, with analytic hierarchy process (AHP), we make a study model which can describe how to set the workforce policies based on the technology development trend.

2. Background

Workforce Planning is to predict the future demand for different types of staff and to seek to match this with supply. The demand is a number of staff required to deliver the planned services using anticipated models of care and the supply is a number and types of people, and skills that are available to be deployed in the delivery of services both now and in the future. Information security workforce who produce and implement information security products, and who is in charge of information security in organizations, has been important. But, estimating the size of the demand for workforce is difficult because it is not a unitary entity. Instead, it is a chaotic amalgam of separate demands with ambiguous boundaries and possibilities of surplus supply or shortage supply always exist.

The causal-loop diagram is a powerful graphic tool to see the relationships among a system's parts and their interactions with each other. Attempting to draw the causal-loop diagram is a useful process for gaining a better understanding of a system's mechanisms and feedback links. Going through a learning process will help us to modify our decision rules and our mental models of the real world. As we get updated in a learning process, we will be able to set dynamic improving goals for the system under study (Forrester, 1961).

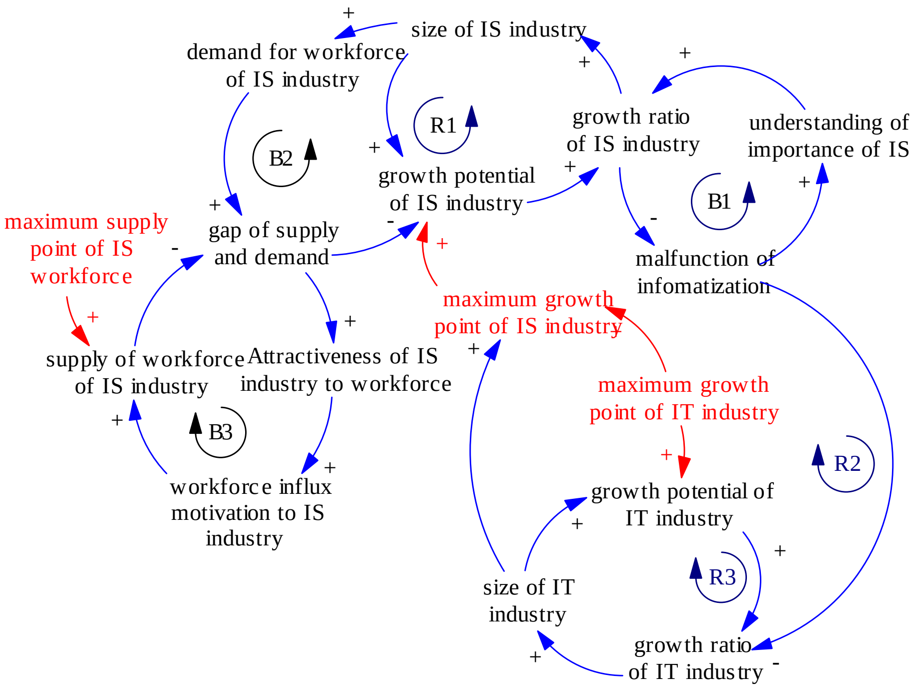
size of IS industry
demand for workforce of IS industry
growth ratio of IS industry
understanding of importance of IS
R1
B2
growth potential of IS industry
B1
maximum supply point of IS workforce
gap of supply and demand
malfunction of infomatization
maximum growth point of IS industry
supply of workforce of IS industry
Attractiveness of IS industry to workforce
maximum growth point of IT industry
B3
R2
workforce influx motivation to IS industry
growth potential of IT industry
R3
size of IT industry
growth ratio of IT industry

Fig. 1. Causal-loop diagram of information security workforce market

*IS: Information Security ** IT: Information Technology
***B: Balancing loop ****R: Reinforcing loop

A causal-loop diagram consists of variables connected by arrows denoting the causal influences among the variables. The important feedback loops are also identified in the diagram. Variables are related by causal links, shown by arrows. Each causal links is assigned by a polarity, either positive (+) or negative (-) to indicate how the dependent variable changes when the independent variable changes. A positive link means that if the cause increase, the effect increases above what it would otherwise have been, and if the cause decreases, the effect decreases below what it would otherwise have been. A negative link means vice versa. The important loops are highlighted by a loop identifier which shows whether the loop is a positive (reinforcing) or negative (balancing) feedback (Sterman, 2000). The attribute of the loop is determined by the numbers of negative link. If the loop has odd numbers of negative links, its attribute is B (balancing feed loop), and if even numbers of negative links, its attribute is R (reinforcing feed loop).

Fig.1 shows causal-loops which generally exist in the information security workforce market. The B1 loop is associated to the formation of the information security industry. It begins with increase of 'understanding of importance of IS' which can cause increase of 'growth ration of information security industry'. And, increase of 'growth ratio of information security industry' can cause decrease of 'malfunction of informatization'. Decrease of 'malfunction of informatization' also can cause decrease of 'understanding of importance of IS'. In result, the polarity of the first link is positive (increase causes increase), the second link is negative (increase causes decrease) and the third link is positive (decrease causes decrease). The R1 loop begins with the increase of 'growth ratio of information security industry' which causes increase of 'size of information security industry'. And, increase of 'size of information security industry' can cause expansion of whole 'growth potential of IS industry'. Expansion of whole 'growth potential of IS industry' also can cause increase of 'growth ratio of information security industry'.

The growth of information security industry is dependent on 'growth potential of information technology industry' because the information security industry is the sub-industry of the information technology industry. These are illustrated by two reinforcing feedback loop in Fig.1 (R2 and R3). The B2 loop is associated to demand for workforce. It begins with increase of 'size of information security industry' which cause increase of 'demand for workforce of information security industry'. And, increase of 'demand for workforce of information security industry' can cause increase of 'gap of supply and demand'. Increase of 'gap of supply and demand' also can cause 'growth potential of information security industry' which can cause increase of 'growth ratio of information security industry'. Increase of 'size of information security industry' again causes increase of 'demand for workforce of information security industry'. At last, B3 loop is associated to supply of workforce. It begins with increase of 'gap of supply and demand' which causes increase of 'attractiveness of information security industry to workforce'. Increase of 'attractiveness of information security industry to workforce' can cause increase of 'workforce influx motivation to information security industry' and this also can cause increase of 'supply of workforce of information security industry'. And, increase of 'supply of workforce of information security industry' can cause decrease of 'gap of supply and demand'

3. Research Model

A typical hierarchy involves representing the overall objective of the decision at the top level, the element criteria affecting the top level (overall objective) including hidden criteria at the intermediate level, and the alternatives at the lower level. In other words, the first level is placed by the objective of the decision making, the second is the criteria and the third is the alternatives.

We make four-level hierarchy model to decide the best workforce training field for information security industry to solve the gap of demand for and supply of information security workforce. As shown in Fig. 2, we make a four-level hierarchy model for this purpose. The six sub-criteria are grouped by three criteria: technical factors, economic factors and societal factors.

In this model, we treat information security technology categories workforce training field, and set as alternatives to decide what the best training field to solve the gap of demand for and supply of information security workforce.

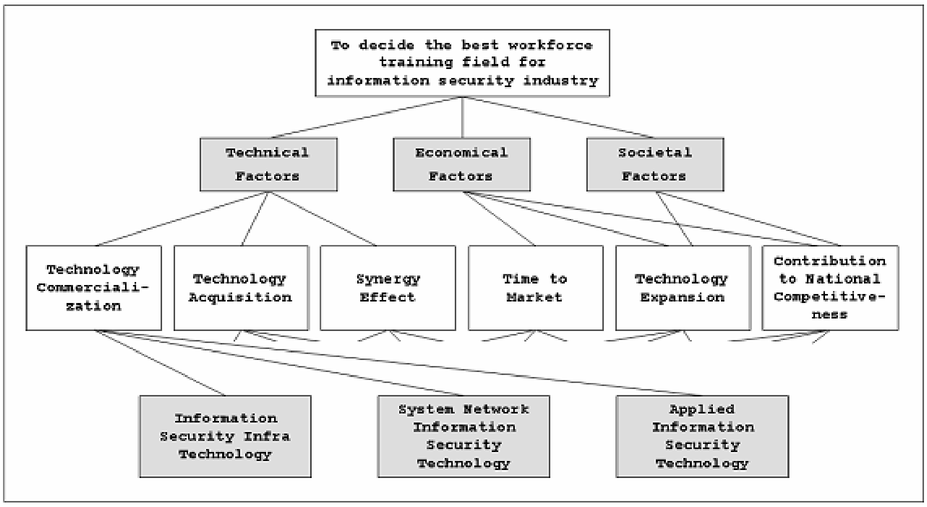
To decide the best workforce training field for information security industry
Technical Factors
Economical Factors
Societal Factors
Technology Commerciali-zation
Technology Acquisition
Synergy Effect
Time to Market
Technology Expansion
Contribution to National Competitive-ness
Information Security Infra Technology
System Network Information Security Technology
Applied Information Security Technology

Fig. 2. The AHP model

3.1. Criteria

We review literatures which investigate the factors for selecting technology category and for adopting the criteria because there is no preceding study on selecting for information security technologies or R&D project, and workforce training field of information security.

Over two hundred qualitative and quantitative models exist in the literature for R&D project selection. Selection models include financial models, checklist models, decision theory models, consensus models, and portfolio models. Brenner (1994) uses AHP for selecting and weighting criteria to select projects. He uses very wide range criteria: portfolio issues, implementation factors, political issues, probability of successes and cost. To select reasonable R&D project, Henriksen and Traynor (1999) uses the criteria of relevance, risk, reasonableness and return. Meade and Presley (2007) uses the criteria of technical, market and organizational issues.

As shown in Fig. 2, we set up three criteria and six sub-criteria from reviewing literatures. The criteria are technical factors, economic factors and societal factors.

The *'technical factors'* are standards to decide workforce training field which can enhance the technical competitiveness of national information security technology. The *'economic factors'* are standards to decide workforce training field which can promote size of domestic information security industry. The *'societal factors'* are standards to decide alternatives which can exalt national people's recognition about importance of information security.

The *'technical factors'* are divided into three sub-criteria: technology commercialization, technology acquisition and synergy effect. The *'technology commercialization'* addresses the degree to which the technology can be commercialized within limited period with limited resources. The *'technology acquisition'* addresses the degree to which the technology can continue everlasting evolution. *The 'synergy effect'* addresses the degree to which the technology can form perfectly new technology by convergence with other technology categories (e.g., information technology).

The *'economic factors'* are divided into three sub-criteria: time to market, technology expansion and contribution to national competitiveness. The *'time to market'* addresses the degree to which the technology can cause steady demand of market. The *'technology expansion'* addresses the degree to which the technology can cause innovative technological evolution and new market. The *'contribution to national competitiveness'* addresses the degree to which the technology can contribute to growth of national economy and acquisition of global competitiveness.

The *'societal factors'* are divided into two sub-criteria: technology expansion and contribution to national competitiveness. The *'technology expansion'* addresses the degree to which the technology can enhance national and societal recognition for importance of information security. The '*contribution to the national competitiveness'* addresses the degree to which the technology can promote national and global competitiveness of information security.

3.2. Alternatives

Under the classification of the ministry of information and communications (MIC), the information security technology is classified into three main segments: fundamental information security technology, system and network information security technology, and application information security technology (MIC, 2002). Also, the ministry of science and technology (MOST) classifies information security technology into two main segments: encryption/ authentication technology, and system and network security technology (MOST, 2002).

As shown in Fig. 2, we adopt MIC's classification as alternatives of the model. The alternatives are workforce training fields which are treated as the best solution can solve the gap of demand for and supply of workforce. The '*fundamental information security technology'* addresses that workforce suppliers, such as colleges, universities, private training institutes, and so on, have to train people who have a specialty in information security infra technology, such as encryption, authentication, electronic signature, PKI, and so on. The '*system and network information security technology'* addresses that workforce suppliers have to train people who have a specialty in system network information security technology, such as firewall, IDS and so on. The '*application information security technology'* addresses that workforce suppliers have to train people who have a specialty in fundamental information security technology, such as electronic payment solution, electronic money system and so on.

4. Analysis and Results

A questionnaire-based field survey is conducted to investigate the relative preference of alternatives on experts of information security industry. The study identifies different relative importance of each criteria and priority of alternative workforce training fields across information security industry. The criteria and alternatives are initially developed based on a literature review. Then, by conducting interviews with experts, wording, content, and format of the questionnaire are modified.

The data were analyzed by using Expert Choice, a software package implementing the analytic hierarchy process. The Expert Choice provides results including local and global weights, priorities for the alternatives, and sensitivity analysis.

Table 3 shows synthesized priorities and rankings of criteria respect to criteria and sub-criteria. As shown in Table 4, the '*technical factors'* criterion has the highest weight of 0.502, followed by the *'societal factors'* (0.334) and the *'economic factors'* (0.163).

Table 4 describes consistency ratio (CR) per each respondent and synthesized results. Also, it shows us relative importance of alternatives. In results, overall CR of the survey result is reported as 0.11 (11%). Followed by inconsistency rule of Saaty, below 20% of inconsistency can be permitted, we can believe that survey result is reliable. As shown in Table 4, the *'system and network information security technology'* is the highest weight of 0.387, followed by the '*application information security technology'* (0.377) and the *'fundamental information security technology'* (0.236).

In conclusion, the most effectual criterion to decide most preferable training field is the *'contribution to national competitiveness'* of the *'societal factors'*, and the least one is the *'contribution to the national competitiveness'* of the *'societal factors'*. And, the '*system and network information security technology*' is chosen as the most preferable training field to solve the gap of demand for and supply of information security workforce.

Table 3. Synthesized priorities and rankings of criteria

criteria	relative importance		sub-criteria	in respect to criteria		in respect to sub-criteria	
		ranking		Relative importance	Ranking	Relative importance	ranking
Technical Factors	0.502	1	Technology Commercialization	0.419	2	0.210	3
			Technology Acquisition	0.157	3	0.079	5
			Synergy Effect	0.424	1	0.213	2
Economic Factors	0.163	3	Time to Market	0.434	1	0.071	6
			Technology Expansion	0.333	2	0.054	7
			Contribution to National Competitiveness	0.234	3	0.038	8
Societal Factors	0.334	2	Technology Expansion	0.250	2	0.084	4
			Contribution to National Competitiveness	0.750	1	0.251	1
	1.000			3.000		1.000	

Table 4. Consistency ratio and relative importance of alternatives per each respondent

section		Respondent 1	Respondent 2	Respondent 3	Respondent 4	**Geometric Mean**
Consistency Ratio (CR)		**18%**	**17%**	**22%**	**4%**	**11%**
relative importance of alternatives	Fundamental Information Security Technology	0.154	0.188	0.185	0.112	**0.236**
	System and Network Information Security Technology	0.388	0.620	0.230	0.363	**0.387**
	Application Information Security Technology	0.458	0.192	0.585	0.525	**0.377**

5. Implications and Conclusions

The studies related with workforce commonly focus on how to control the quantity of workforce. Because many studies and policies about workforce training have analyzed how to increase the supply, only surplus or shortage supply problem exist in workforce market. The Korean government has implemented various policies to promote the information security workforce. Those policies have been successful to supply enough number of workforce, but not successful to meet the various requirements of the demand.

The purpose of this study is to investigate possibilities of qualified workforce training which can be the solution itself to meet the demand of industry and can cause no surplus or shortage at any part of the industry. We suggest the direction of workforce training policies of information security industry through investigating this purpose with questionnaire-based field study adopting analytic hierarch process. With investigation, we recognize that workforce demanders of the industry already understand necessity of workforce policies to train qualitative workforce. And, the '*system and network information security technology*' is recognized as the most preferable workforce training field by respondents. The meanings of this result can be interpreted as the market-driving field of information security industry at this time is the services and products which are based on *system and network information security technology*.

References

Brenner, M.S. (1994), Practical R&D Project Prioritization, *Research Technology Management*, 37, 38-42.

Byun, D.H. (2001), The AHP Approach for Selecting an Automobile Purchase Model, *Information & Management,* 38, 289-297.

Forrester, J.W. (1961), *Industrial Dynamics*, MIT Press.

Henriksen, A.D. and Traynor, A.J. (1999), A Practical R&D Project-Selection Scoring Tool, *IEEE Transactions on Engineering Management*, 46, 158-170.

Jiang, J. and Klein, C. (1999), Information System Project-Selection Criteria Variations within Strategic Classes, *IEEE Transactions on Engineering Management*, 46, 171-176.

Lee, M.S. and Om, G.Y. (1996), Different Factors Considered in Project Selection at Pubic and Private R&D Institutes, *Technovation*, 16, 271-275.

Meade, L.M. and Presley, A. (2002), R&D Project Selection using the Analytic Network Process, *IEEE Transaction on Engineering Management*, 49, 59-66.

MIC (2002), *National R&D Plans for the Information Security Industry*. (in Korean)

MOST (2002), *National Technology Roadmap* (in Korean)

NCA (2005), *2005 National Informatization Whitepaper* (in Korean)

NIS (2005), *2005 National Information Security Whitepaper* (in Korean)

Saaty, T.L. (1995), *Decision Making for Leaders*, RWS Publications.

Sterman, J.D. (2000), *Business Dynamics*, McGraw-Hill.

Vargas, L.G. (1990), An Overview of the Analytic Hierarchy Process and its Applications, *European Journal of Operational Research*, 48, 2-8.