The Analysis of Causal Relation Factors about Investment of Government in Information Security Industry

Hee-Kyung Kong
Department of MIS, Chungbuk National University
#12 Gaeshin-dong, Heungdeok-gu, Cheongju, Chungbuk, 361-736, South Korea
Tel:+82-43-276-3343/Fax:+82-43-273-2355 konghk@paran.com

Tae-Sung Kim
Department of MIS, Chungbuk National University
#12 Gaeshin-dong, Heungdeok-gu, Cheongju, Chungbuk, 361-736, South Korea
Tel:+82-43-261-3343/Fax:+82-43-273-2355, kimts@chungbuk.ac.kr

Abstract. *In this paper, we use to system thinking analyze the outcome drawn by the increased government investment in information security industry. We also analyze the structure of the feedback, derived from the inter-connection of diverse variables that affects the investment for information security industry by both public and private sectors. Moreover, this study would help to establish incentives that would resolve problems related on information security.*

Keywords: information security, government investment, system thinking

1 Introduction

There has been a rapid growth in the field of information technology, which has caused an explosive growth of internet usage. As we live in a high-tech era, more interest and focus have been given to individuals' capacity to collect and use information. This capacity plays an important role in competition among individuals, companies and countries. On the other hand, the rapid progress of information technology has yielded serious side-effects, such as the invasion of privacy, the destruction of information system, and so on. The threat of such side-effects has reached a point where they have caused prodigious losses to

the country. Therefore, there has been an increasing awareness in the importance of information security (IS). Consequently, information security has become an imminent agenda not only on the sphere of individuals' interest but also of countries' interest. Information security involves the effort to keep information safe, preventing it from being illegally released, falsely transformed or destroyed. So, in order to resolve such problems it is essential to keep putting an effort to develop technology, approaching this matter through the angle of socioeconomics.

1.1 Socioeconomic Research on the Investment for the Information Security

It is expected that there would be an increasingly more active research on the issue of information security through the angle of socioeconomics. First, as insurance industry is likely to deal with this matter with utmost interest, there would be an increasingly more precise research on the effect of information security, including the research on the loss and the prospect for the gain. Second, it is fundamentally important for the government and enterprises to have enough budgets for this information security project. Third, it is expected that there would be more discussions on the appropriate amount of investment along with the estimation of the effect of the investment so that information can be effectively protected on the level of individuals, companies and countries according to the free market logic [8]. Therefore, various economic models have been studied for information security issues. For example, some researchers use net present value models and game theory to derive the optimal amount of investment. Some apply economic theories to the matter of sharing information [1][2][3]. As sharing information among companies increase due to the change in the business process, a Japanese researcher analyzed the effect of the investment for information security in relation between vulnerability and information security investment in the structure of sharing information among companies [10]. The investment for information security on the public sector involves a complex coordination among the recognition of its urgency, insuring enough budgets, establishing law and maintaining experts, who can operate this project. Private sector investment for information security also has a complex, systematic characteristic, involving specialization of business, investment for developing technology, rais-

ing experts, and insuring the quality of products as well as service in the market of information security, which would fit into the free market logic. We derive the dynamic relationship between the investments by the public and private sectors through a diagram in order to find the appropriate amount of investment to the information security market.

We think that the conventional research in this matter has done with an exclusive consideration on the growth and expansion of information security industry. Therefore, it lacks knowledge about the complex relationship among diverse variables and fails to reflect it to make a more solid system of information security due to government's protective investment which banned competition.

In this paper, we analyze it, using the system thinking. First, we show the changes in the side effects of technology such as hacking and virus infection. Second, we analyze the changes in the feedback structure that affects the investment for information security on the part of the public and private sectors. Third, we consider the probable delay that can occur through a conflict among diverse factors. Finally, we analyze the organic structure of relationship among factors dealing with the information security industry done by the government and by individual companies respectively.

2 Current Situation of Information Security Industry

2.1 Information Security System and Introduction of the Industry

The information security system is a system which enables one to protect one's own information system and the content of information by a proper and consistent management of information security products such as hardware and software [4].

However, the rapid progress of the technology that is used illegally to inflict other information security system yielded the demand for a market which provides information secure services. Thus, this service is included in the range of information security system. Therefore, information security industry is considered a major industry that develops and provides information secure products and services as well as a consistent management of products and services.

In order to conceive the level of the capacity of information security it is necessary to classify IT security spending, manpower and the size of industry into two categories: the government and the individual companies. In fact, Korea's IT security spending for this matter is very

low compared to other advanced nations such as America. To be able to see how much more IT security spending is required we need to examine the current IT security spending. We can see Korea's IT security spending for advancing information technology knowledge in comparison with the IT spending for information security in the following Table1 [6][7].

Table 1. IT Security spending / IT Spending(unit:hundred million won)

Classification	2001	2002	2003	2004	2005
IT spending	15,029	16,114	16,380	16,546	20,707
IT security spending	259	306	368	414	1,036
IT security spending / IT spending	1.7%	1.9%	2.2%	2.5%	5.0%

Korea's IT security spending is gradually increasing. Yet it is still very low. America's IT security spending was 2,700,000,000 dollars in 2002, which is 5.6% of the whole IT spending, 48,000,000,000 dollars. In 2003, it was 4,600,000,000 dollars, which takes up 8.8% of IT spending, 52,000,000 dollars [5][6][7]. Other advanced nations have IT security spending in average 8-10% out of the whole IT spending. Korea's IT security spending is only one fourth to one half that of these countries.

The fact that the percentage of Korea's investment for information security is below 5% out of the whole IT spending for information technology may yield lots of potential problems. It would not matter if we get good effects out of the relatively small investment. However, it does not work that way. Currently Korea has become one of the most advanced internet using countries; there are 25,000,000 internet users, indeed, 67% of stock market trade is done through internet and there are many business, and bank exchanges, done by using internet. In January, 2003 when Worm Virus was spread all over the world, Korea suffered from the virus more than any countries. This instance reveals the fact that Korea did not invest enough to prevent such damage.

Moreover, Korea's manpower and the capacity of dealing with such matter are evaluated negatively. Thus it is imminent to supply more manpower so that each organization and company could manage such matter to enhance the level of the capacity of protecting information. We can see the current situation of the supply of manpower in the Table 2 [6][7].

Table 2 The current situation of the supply of manpower (unit: man)

Classification	2002	2003	2004	2005
IS R&D	1,506	1,824	2,164	1,901
IS Management	559	768	924	1,405
IS Products & Service Sales	-	-	386	663
Etc	1,048	1,341	532	364
Total	3,018	3,933	4,006	4,333

2.2 Factors to be Considered for Investment for Information Security Industry

The basic factors of information security consist of confidentiality, integrity, availability, authentication, access control and so on [3]. In the process of fulfilling these factors there might be conflict among factors and much expense is needed. Therefore, it is necessary to recognize the importance of establishing an information system and to estimate possible loss due to the lack of solid information protective system that can exterminate or reduce damage by illegal activities using high technology, so that an appropriate level of investment for information security could be drawn. To protect information intact we need to have data that show the appropriate amount of budget and investment, accurately estimating how much expense is needed to establish an information system. However, there is not enough research on deriving data concerning investment for information security based on logic or a theory. Exclusive focus on economic analysis from the view point of companies would entail a limitation of not being able to reflect the lurking dangerous factors, which exist in reality.

3 Dynamic Analysis of the Structure of Information Security Industry

In this research, we present a causal loop in order to clearly analyze the relationship among various factors of feedback structure and its movement, so that we can accurately analyze the appropriate amount of investment. Causal loop is the most important tool that enables us to understand the feedback structure in a system by letting us see it in two-dimensional space. In causal loop, arrows are used to indicate the direction of causal relations among variables. Secondly, along with arrows, marks such as (+) and (-) are used to indicate directions of the causal relations. If the relations among variables face toward the same

direction, for example increase → increase, then it has a positive (+) relationship, if it is increase → decrease then, it has a negative (-) relationship. Third, when various causal relations form a confined circle, it is called as feedback loop. If the relation among variables contains even numbers of (-) in the whole loop, R is used to mark "Self-Reinforcing", if there is odd number of (-) then, B is to be marked, indicating "Self-Balancing" [9].

We introduce some definitions to explain the concept of the investment for information security by the government. The investment for information security by the government, which is based on the informatization spending, refers to the assistance for raising manpower and developing technology and increasing information security industry sales.

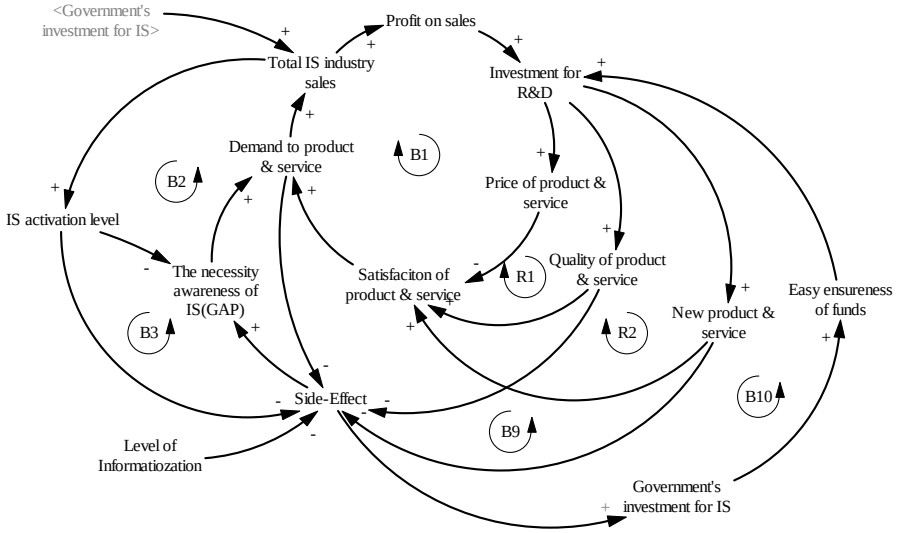

Fig. 1. Government investment for R&D and IS industry sales

Like R1, in R2 we can also see that the investment for developing technology knowledge induces making new products and services. And the expanded demands. Furthermore, the expanded demands increase the information security industry sales and profit that made virtuous cycle for strengthening 'Investment for R&D'.

In R1 loop, we see that the government's investment for information security yields improvement of the quality of products for information security. The improvement of the quality of the products and related

service satisfies customers. In return, there come more demands for such products and service, which lead to the increase in the profit and the number of companies.

B1 loop shows how the investment for developing technology on the part of companies, done based on free market logic, plays a role to increase the manufacturing expense, which entails the increase of the price of products, decreasing demands. Increasing Information Security industrial sales causes frequent activation of information security. It also could reduce side effect and demand of products and service along decreasing information security cognition. Also, the financial problem which is teasing all the companies, is solved by government's IS investment policy mainly and it promotes enhancing quality of product and service and helps forward new products on the markets.

Therefore, in order to bring improvement of information security industry, diverse efforts, such as innovation of the quality of products on the part of companies, creation of more demands, and reconsideration of price competition, are essential.

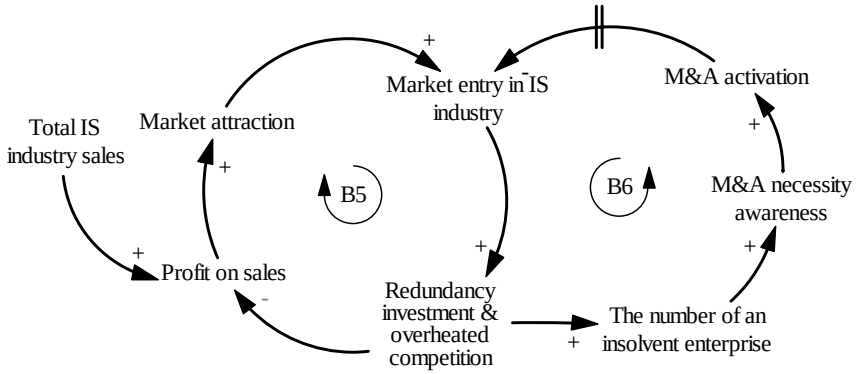

Fig. 2. M&A activations loop

In B5 and B6, we can see that the overall scale of information security industry has increased [5]. However, the decrease of the investment of the government yields the decrease of profit in companies due to an intense price competition among companies. Thus, eventually it creates vast number of companies that are in financial trouble. This phenomenon reveals the imminent necessity for M&A, which has been raised consistently by people, involved in the information security industry. It

is because that M&A would produce synergy and reinforce the power for competition.

Additionally, it is also indispensable for the government to support this industry through financial assistance and persistent policy. As we see so far, information security industry requires a consistent and positive aid to ensure the security of environment of information. Thus, unlike other industries, information security industry is a key industry. Such characteristic of information security industry shows that it contains a system that has a very complex and strong movement, related with IT industry.

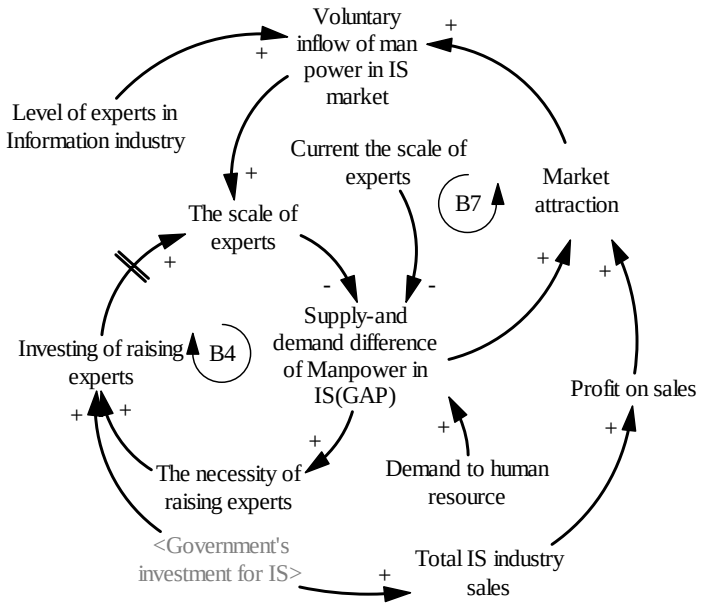

Fig. 3. Government investment for raising experts

The government investment for raising manpower means providing education to raise experts in the field of technology knowledge, imbuing them with the necessity of protecting information(B4). The gap between the demand and the supply of manpower, and the relationship among variables in the government's investment reveal that the government's investment for information security plays a significant role in the plan of modulating the supply of manpower. Moreover, reducing the gap between the demand and supply of manpower would bring

about increase of degree of consumers' satisfaction about products of information security.

In short, the government's investment would induce a decrease in the gap between the demand and supply of manpower and an increase in the demand for information security products and services.

Bigger gab between demand and supply of the information security staff makes higher scarcity of the staff and it also increases needs of the new and experienced the staff and that makes a natural in draft staff into the market.

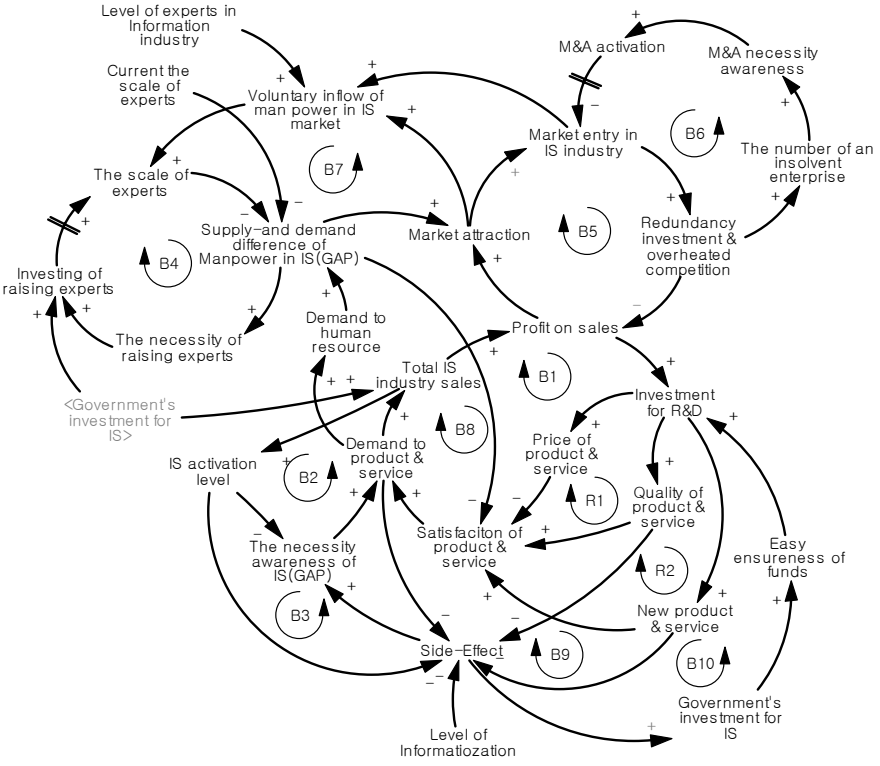

Fig. 4. Structure of information security industry and the dynamic relationship among variables

Eventually, it bring about a balanced structure in the information security industry because it would reduce hacking activities, and cause a decrease in the level of recognition of the necessity for information

security, which would induce a decrease in the demand for the products of information security and related services(B8).

In this causal loop, we can analyze the structure of the relationship among variables, finding causal factors between the amount of products and service in the market of information security and the relationship between the information security industry, supported by the government and individual companies, as well as the level of activation of information security, derived from the investment for information security.

It is very dangerous to attempt to predict the future of the information security industry through only a few data and simplistic thinking. Especially the industries dealing with high technology knowledge have a characteristic of having much room for various possibilities in the way for the variables to be applied. Thus simple analysis of a few data can lead to a fallacy. Therefore, it is desirable to analyze the causes and effects of various factors, reflecting the feedback of factors and the delay of information and material.

4. Conclusion

4.1 Political Implications

In the information security industry, investment by government is very important. We used system thinking to figure out analyze the outcome drawn by the increased government investment in information security industry. We derived consensus of policy.

First, information security industry is by any means an industry in a narrow sense as we think of other industries in general. Considering the effect of information security industry that will affect even other general industries that do not have much to do with IT industry, it makes a lot of sense for the government to invest on information security industry with more active and persistent attitude and more keen realistic sense. In addition to that, it is also required for individual companies to actively participate in the investment for the bright future of information security industry.

Second, the investment by government on information security industry should be done with a changed attitude from action by forecasting to action by learning. In order to do so, we need to establish precise and profound knowledge-based information systems so that we can make global optimization possible instead of local optimization.

Third, we need to establish a flexible structure of the investment for information security industry by government in order to respond quickly to the changing situation of information security industry. Even though we cannot really be free from the limitation of insufficient budget, we need to overcome it and to try to establish a smooth stream like chain of value.

Fourth, in order to get rid of uncertainty and insecurity in the information security industry, it is necessary to make a balance between government participation and individual companies' participation, between demand and supply, and technology knowledge and policies. It is because that only through joint and cooperative effort from both parties we can establish a solid and productive information security industry.

4.2 Future research

It is necessary to discover more concrete factors as well as to proceed into researches that take a diverse group of customers into consideration. In addition to extending our model as suggested above, there is much room for further research in the area of excavating objective, realistic principle of investment for information security industry by government.

References

1. Gordon, L.A. and Loeb, M.P., "The economics of information security investment," ACM Transactions on Information and System Security, Vol.5, No.4, pp.438–457, 2002.
2. Gordon, L.A, Loeb, M.P. and Lucyshyn, W., "An economics perspective on the sharing of information related to security breaches." Proceedings of WEIS, UC Berkeley, 2002.
3. Gordon, L.A. and Richardson R., "The new economics of information security," Information Week, Issue 982, pp.52–57, 2004.
4. Jeon, Jaeho, "A dynamic analysis on the relative effectiveness of promoting policies for information security industry," The Journal of Korean System Dynamics, Vol.4, No.2, pp.5–44, 2003.
5. National Computerization Agency, National Informatization Whitepaper, 2005 (in Korean).
6. National Intelligence Service, National Information Security Whitepaper, 2004 (in Korean).
7. National Intelligence Service, National Information Security Whitepaper, 2005 (in Korean).

8. Shin, Ilsoon, “Review the economics means to information security,” Information Security Review, pp.27–40, 2004.
9. Sterman, J. D., Business Dynamics: System Thinking and Modeling for a Complex World, Irwin McGraw-Hill, 2000.
10. Tanaka, H., Matsuura, K. and Sudoh, O., “Vulnerability and information security investment: An empirical analysis of e-local government in Japan,” Journal of Accounting & Public Policy, Vol.24, No.1, pp.37–59, 2005.