An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan

Wei Liu * Hideyuki Tanaka * Kanta Matsuura *

Abstract— This paper presents a two-step empirical analysis of investing in security countermeasures based on an Japanese enterprise survey. At the first step, we verify the relations between probability of computer virus incidents and adopting a set of information security countermeasures. It is shown that "Defense Measure" associated with "Information Security Policy" and "Human Cultivation" has remarkable effects on virus incidents. At the second step, we analyze the effect of continuous investments in the three security countermeasures using two years' data. The empirical results suggest that virus incidents were significantly reduced in those enterprises which adopted the three countermeasures both in 2002 and in 2003.

Keywords: Information security (IS) investment, IS incident, IS countermeasure, Empirical analysis, Countermeasure complementarity, Continuity of IS investment

1 Introduction

With the rapid growth of organizations' dependence on information systems, particularly Internet, the issue of information security (IS) draws more and more attention. Unfortunately although security technologies have made a great progress in past decades, security level almost has never been improved [1]. Resent researches clarify that security is not only a technology problem but the matter of economic incentives for information security investment, so the focus is shifting from what is technically possible to what is economically optimal [2, 3].

To inspire managers to concentrate on security risk management, some studies documented status of IS and potential losses due to security breaches [4, 5], and others showed return on security investment (ROSI) to convince managers about the benefits of security efforts [6, 7, 8]. Besides these qualitative studies, researchers are engaged in quantitative studies as well. An economic model that determines the optimal security investment to protect a given information set was proposed by Gordon and Loeb in 2002 [9]. Based on the Gordon-Loeb model, Tanaka and Matsuura conducted an empirical analysis using data on e-local governments in Japan and verified the relation between vulnerability and information security investment[10]. The contribution of their research is not only supporting a prior study, but implying the importance of empirical studies as well.

Above mentioned researches indicate a direction for organizations: they should improve security status by improving the ROSI in security management process. However, managers still have no idea about how to gain the optimal ROSI. To have an insight into the black box of security management, managers should exactly know two factors: the IS threats facing their

* The University of Tokyo.

information assets and the valid countermeasures against those threats. The two factors are essential opposite factors of security risk analysis. More importantly, they should know how to appropriately invest in countermeasures to defend against security incidents effectively and efficiently [11]. Some researches, just like in [1, 4], use figures and rankings to identify the actual threats and present available countermeasures. Other ones provide security management methods and generally prove the efficiency of their methods by conducting a case study in a company or other organizations [12, 13, 14, 15, 16].

When talking about investment, people are apt to consider tangible assets. However, recent researches show that the complementarity of investments in tangible assets and intangible assets (just like personnel training, corporate culture and so on) can raise productivity and bring enterprises greater profit [17, 18, 19]. This theory is hold good for IS investment. Tanaka introduces the concept of intangible assets into IS investment and approved the complementarity between tangible and intangible assets might work in IS investment [20].

These prior researches conduce to security management for enterprises and give us a hint to verify the effects of complementarity of security countermeasures. Furthermore, literature which discusses the effects of continuous investments in countermeasures does not exist, neither does rigorous empirical study. Given this situation, we conducted an empirical analysis based on an enterprise survey in Japan. The results of our study not only show the great importance of countermeasures complementarity but suggest that continuity of security investments in countermeasures has positive effect on improving enterprises' security status.

The remainder of the paper is organized as follows. Section 2 gives a review of the status of IS incidents and countermeasures. Section 3 covers the research design, our hypotheses and regression models. In the same section, we discuss the empirical results and their implications as well. In the last section, conclusions and future work are detailed.

2 IS incidents and countermeasures

2.1 IS incidents

Knowing the enemies facing information security is a vital component to shaping an information security defense posture. In order to strengthen the level of protection of information in the enterprises, those responsible for information security must begin with an understanding of the threats facing their information assets, and then they could establish security strategies accordingly [1].

The 2005 Computer Crime and Security Survey conducted by Computer Security Institute and Federal Bureau of Investigation (CSI/FBI) [4] gives a shocking report that the percentage of respondents answering that their organization experienced incidents in the last 12 months is 72%, and the total losses for 2005 due to security breaches were $130,104,542. Among all the categories of incidents, "Virus" gets the top in the losses ranking as usual, with a $42,787,767 losses. "Unauthorized Access" and "Theft of Proprietary Information" are the second and the third places. The three categories swamped the losses from all other categories. This can be explained by the increased awareness of, and improved technology to cope with some threat types, such as "Virus".

Similar results are presented in "Survey of actual condition of IT usage" conducted by METI (Ministry of Economy, Trade and Industry) of the Japanese government in 2003 [21]. The top 2 categories in proportion ranking of incidents are "Insider System Trouble" (27.1%) and "Computer Virus" (26.1%). Although losses due to incidents are not concerned in this survey, we can still see that the two categories incidents are far more critical than other ones both in terms of incident rate and incident severity denoted by breakdown times in systems.

2.2 IS countermeasures

Based upon the understanding of the primary threats to enterprise information, security managers should decide appropriate defenses in the next step. In this article, we discuss countermeasures by which aspects they focus and center our attention on three categories of generally adopted countermeasures: "Defense measures", "Security policy", and "Human cultivation". As the responsibility of security management for enterprise, security managers must be familiar with the critical components of security countermeasures.

"Defense measures" are considered the primary technology addressed systems defending against network attacks. Firewall, the delegate of defense measures, is simply a perimeter defense device that splits a network into trusted or protected, and un-trusted or unprotected side elements [22]. In CSI/FBI survey, use of firewall was reported by 97 percent of enterprises and anti-virus software was reported as being used by 96 percent of the respondents. It is clear that enterprises lay particular stress on defense measures.

"Security policy" defines the security philosophy and postures the organization takes, and is the basis for all subsequent security decisions and implementations [1]. It is indicated that security policy would be part of the security standards, procedures, and guidelines. A well-designed and maintained security policy potentially can reduce costly forays, as well as provide protection from disaster [23].

Another fundamental part of an organizations security function is the implementation of a security education, training, and awareness program. Security researchers warn that information security continues to be ignored by top managers, middle managers, and employees alike. Enterprises should conduct education and training that will inform their employees of what happens if the security policy is not followed and instruct employees in specific actions that need to be taken to protect against security violations [22]. Furthermore, security managers of enterprises have a significant role to play in engineering desirable organizational security level through proper planning and reasonable resource allocation.

Both security policy and human cultivation are relatively low-cost protection mechanisms with the potential for high ROSI, however, many studies indicate that enterprises often overlook policies and the human solutions, when in fact the two factors must be addressed first, with technology assisting in the enhancement for security [1, 24].

3 Models

3.1 Data

The data of our analysis is based on "Survey of actual condition of IT usage", conducted by METI (Ministry of Economy, Trade and Industry) of the Japanese government in March 2002 and 2003. To grasp the information processing state in Japanese enterprises, METI conducts this survey annually. All the Japanese nongovernmental enterprises making use of computers and information services are the survey objects. In each of the two years 9500 enterprises were randomly chosen by METI and received questionnaires by mail. 5357 firms in 2002 and 4491 firms in 2003 handed in their answers. To verify the effects of countermeasures complementarity and continuous investments in security countermeasures, we matched the data of 2002 and 2003 and chose all of the 3018 enterprises which are on the both company lists as our analysis objects.

From the survey, we used the data which are considered to be important organizational factors related both to security incidents and to companies' decisions on security investments. The data are as follows:

- the number of e-mail accounts,
- industry type,
- network structure,

and

- system coverage

in every enterprise. Of course, in order to examine the effectiveness of information security investment, we need to use the data of IS incidents and countermeasure adoption, too.

3.2 Step1 for verifying the effectiveness of countermeasures complementarity

3.2.1 Former study

As mentioned in section 2, as a result of enterprises increasingly relying on information systems and networks, external attacks are being the leading threats to enterprises for many years, especially "virus" is the source of the greatest financial losses. Given this situation, we focus our attention on "virus" and want to make it clear that what countermeasures are effective for virus incidents and should be invested. In our former study reported at a Japanese domestic symposium [25], we verified the relations between probability of computer virus incidents and adopting information security countermeasures by analyzing the 2003's survey data. The empirical results suggest that "Defense Measure" associating with "Information Security Policy" and "Human Cultivation" could significantly reduce virus incidents, whereas enterprises relying on defense measures without attaching importance to the other two countermeasures can not enhance their immunity from virus. Before verifying the effectiveness of continuous investments in "Defense Measure", "Information Security Policy" and "Human Cultivation" at the next step, we should examine our former study results by the matched data of 2002 and 2003 of 3018 sample enterprises.

3.2.2 Model1

Logistic regression is a widely used statistic method which fits nominal Y responses to a linear model of X terms. To be more precise, it fits probabilities for the two response levels using a logistic function. We use logistic regression analysis to examine the explanatory ability of explanatory variables (organizational factors and countermeasures adoption) for explained variable (probability of virus incidents) by the following proposed model.

$$Virus_{mi} = \alpha \ln Email_i + \beta SysV_i + \gamma_1 Industry_{1i} + \cdots + \gamma_{26} Industry_{26i} + \delta DPH_i + \epsilon_i (1)$$

where $i = 1, 2 \cdots n$.

* D:Defense Measure P: Information Security Policy H:Human Cultivation

$Virus_{mi}$: virus dummy indicates whether enterprise i has suffered virus attacks in 2003. If enterprise i has such experience, we set the variable 0, otherwise the value of the variable is 1.

ln$Email_i$: natural logarithm of the e-mail account number in enterprise i.

Since e-mail attachment is the top virus source, we use the number of e-mail accounts in a firm to substitute for the vulnerability arises from inside users. The fact that issuing more e-mail accounts exposes the information system to virus more has been verified in Tanaka and Matsuura's empirical work [26].

$SysV_i$: system vulnerability score of enterprise i.

System vulnerability score denotes the degree of vulnerability inhering in system. The more an enterprise extends the coverage of systems and networks, it has the higher vulnerability to threats. Therefore, we calculate the $SysV_i$ for every enterprise using Table 1.

Vulnerability score of every subsystem with different type denoted as the product of system coverage point (1 to 4) and network structure point (1 to 3), and the total vulnerability score of an enterprise is the sum of all subsystem scores. Accordingly, the range of system vulnerability score $SysV$ is between 1 to 72.

$Industry_{1i}, Industry_{2i}, \cdots, Industry_{26i}$: industry type dummies.

We use the industry dummies to denote the industry type of every enterprise. In our former study, we proposed a model to verify the relations between probability of computer virus incidents and adopting information security countermeasures without thinking industry type. Through the further survey, we found that IS investments are significantly affected by industry types [27]. In fact, financial organizations seem to invest more in IS compared to other organizations because they have larger potential losses that may occur from IS abuses [28]. So we improved our model by adding industry dummies to control the influence exerted from industry

Table 1: System coverage and network structure

System Type	System Coverage				Network Structure		
	Within Department	Within Enterprise	Within Related Enterprises	Enterprises Crossing	Intrenet	Outside network	Internet
Basic System	1	2	3	4	1	2	3
Production/Distribution Control System	1	2	3	4	1	2	3
Design/Manufacture Control System	1	2	3	4	1	2	3
Information System	1	2	3	4	1	2	3
New Strategy System	1	2	3	4	1	2	3
Other Systems	1	2	3	4	1	2	3

type. According to the questionnaire, there are 27 types of industries including 14 manufacturing industries and 13 non-manufacturing industries (an industry list appears in the appendix).

DPH_i: dummy of countermeasures adoption in enterprise i.

D,P and H represent "Defense measures", "Security policy", and "Human cultivation" respectively. This variable is binary, if an enterprise adopted all of the three countermeasures, we set DPH 1, otherwise we set it 0.

When choosing explanatory variables for regression model, we should be sure that they are independent. We checked the independence of all explanatory variables of our model and showed their correlation coefficients in the following table.

Table 2: Correlation coefficients of explanatory variables

	ln$Email$	$SysV$	DPH
ln$Email$	–	0.366	0.212
$SysV$	0.366	–	0.154
DPH	0.212	0.154	–

The fact that all the correlation coefficients are far less than 1 means the explanatory variables of our model are independent of one another. Although we did not include the 26 industry dummies in Table 2 due to the limitation of paper, each of them is independent of other explanatory variables according to our examination.

3.2.3 Data process and descriptive statistics

As we use natural logarithm of e-mail account number as controller for the proposed regression, we exclude those enterprises which have no e-mail account. Based on our calculation, the minimum of $SysV$ is 1, so that an enterprise scoring 0 means it may not have constructed system or network. Furthermore, those enterprises which have no domain name are thought to be making a limited use of Internet. Since our research purpose is to examine the countermeasures effects on external security incidents, the enterprises that have extremely low vulnerability and have little contact with external world must be excluded from the sample. Accordingly, there are 2168 enterprises satisfying the following requirements:

- Their e-mail account numbers are not 0.
- Their system vulnerability scores are not 0.
- Their domain names are registered.

Outliers are observations that are unexpectedly different from the majority in the sample which have a strong influence on the calculation of statistics, so 139 enterprises were excluded from our sample because of containing abnormal values in e-mail account number or system vulnerability score. Consequently, the number of total enterprises narrowed to 2029.

The statistics of organizational factors, e-mail account number and system vulnerability score, are as Table 3 shows.

Table 3: Organizational factors

Organizational Factor	Mean	Standard Deviation
Email account number	1206	17596
ln$Email$	4.79	1.95
$SysV$	9.92	7.91

Table 4 shows how many enterprises suffered losses from computer virus, and Table 5 presents the status of countermeasure adoption in the sample enterprises.

Table 4: Experience of virus incident

	No. of Enterprises	% of Enterprises
have experience	1247	57.5%
have no experience	921	42.5%

From Table 4 we can see that more than a half of our sample enterprises have incurred losses due to virus attacks, and the survey results indicates some of the respondents even have more than one hundred times of such experience.

Table 5: Status of countermeasure adoption

Countermeasures adoption	No. of Enterprises	% of Enterprises
adopted the three countermeasures	823	37.96%
others	1345	62.04%

As shown in Table 5, there are about 38 percent enterprises not only implemented defense measures, but also drew up security policies and cultivated their employees. These enterprises are considering the complementarity of the three sorts of countermeasures.

3.2.4 Results of model1

We applied logistic regression analysis to all 2029 enterprises using proposed regression model1. As showed in the Table 5, that P value of whole model test is less than 0.0001 implied the model as a whole to be significant. The analysis results of the parameters in regression model1 are listed in Table 6 as well.

Table 6: The results of the logistic regression analysis of model1

Item	Estimates	Standard Error	ChiSqure	P(Prob>ChiSq)
Whole model test	–	–	291.92	<.0001
Intercept	-1.025	0.244	17.65	<.0001
α (ln$Email$)	0.260	0.032	64.40	<.0001
β ($SysV$)	0.022	0.009	6.11	0.014
δ (DPH)	-0.222	0.110	4.07	0.044

From Table 6, we can see δ, the coefficient of variable DPH, is statistically significant (P value<0.05). The fact that its estimate has a negative sign indicates the explained variable increases by the explanatory variable's decrease. That is to say, adopting three of "Defense Measure", "Information Security Policy" and "Human Cultivation" reduces virus incidents significantly. That ln$Email$ and $SysV$ have positive significant coefficients means more e-mail accounts and higher system vulnerability score involve higher incidence of computer virus. The results strongly support our former study conclusion that installing defense measures with drawing security polices and cultivating employees is effective for computer virus.

3.3 Step2 for verifying the effectiveness of continuous investments in countermeasures

3.3.1 Hypotheses

At the first step, we confirmed that the complementarity of countermeasures is important to defend against virus incidents. And then we made a further consideration wondering whether

there are some differences between continuous investments and single period investments in the three countermeasures regarding computer virus incidents. Based on the obtained data of the years 2002 and 2003, we will verify the effectiveness of continuitiy of security investments at the next step. There are 3018 enterprises which are included both in the year 2002's company list and in the year 2003's company list. The 3018 enterprises can be divided into four classes. The enterprises in the first class adopted the three countermeasures in 2002 and 2003; we regard this adoption in both of the years as continuous security investments. The second class adopted the three countermeasures only in 2003 and the third class invested only in 2002; both of the two classes made single period investments. The last class is composed of the enterprises that did not adopt all the three countermeasures in both years.

In order to examine our wonder (*i.e.*, to verify the effectiveness of continuous security investments), we describe the following two hypotheses:

H1: Continuous investments in "Defense Measure", "Information Security Policy" and "Human Cultivation" could significantly reduce virus incidents.

H2: Single period investments in "Defense Measure", "Information Security Policy" and "Human Cultivation" could not significantly reduce virus incidents.

3.3.2 Model2

We used the following regression model to test our hypotheses:

$$\begin{aligned} Virus_{mi} &= \alpha' \ln Email_i + \beta' SysV_i + \gamma_1' Industry_{1i} + \cdots + \gamma_{26}' Industry_{26i} \\ &+ \delta_1 YY_i + \delta_2 NY_i + \delta_3 YN_i + \epsilon_i' \end{aligned} \tag{2}$$

where $i = 1, 2 \cdots n$.

The variables in this model are the same as in model1:

$Virus_{mi}$: virus dummy indicates whether enterprise i has suffered virus attacks in 2003.

$\ln Email_i$: natural logarithm of the e-mail account number in enterprise substitutes for the vulnerability arising from inside users.

$SysV_i$: system vulnerability score of enterprise i denotes the vulnerability of systems and networks.

$Industry_{1i}, Industry_{2i}, \cdots, Industry_{26i}$: industry type dummies.

YY, NY and YN: investment pattern dummies.

Y means that an enterprise adopted all of "Defense Measure", "Information Security Policy" and "Human Cultivation", whereas N means "not". The three variables are binary, and at most only one of them could be 1 at the same time. If an enterprise adopted the three countermeasures both in 2002 and in 2003, we set $YY = 1$. If an enterprise adopted the three countermeasures only in 2003, we set $NY = 1$. If an enterprise adopted the three countermeasures only in 2002 we set $YN = 1$. Finally, if an enterprise did not adopt all of the three countermeasures in both years, we set $YY = NY = YN = 0$ (such enterprise belongs to the fourth class "NN").

Table 7 shows the amounts and the proportions of the four classes enterprises, and Table 8 presents the correlation coefficients of explanatory variables of model2.

Table 7: No. and % of the four classes enterprises

	No. of Enterprises	% of Enterprises
YY	437	21.0%
NY	357	17.2%
YN	162	7.8%
NN	1123	54.0%

Table 8: Correlation coefficients of explanatory variables

	ln$Email$	$SysV$	YY	NY	YN
ln$Email$	–	0.366	0.186	0.073	0.034
$SysV$	0.366	–	0.125	0.063	0.021
YY	0.186	0.125	–	-0.233	-0.152
NY	0.073	0.063	-0.233	–	-0.133
YN	0.034	0.021	-0.152	-0.132	–

3.3.3 Results of model2

In the same manner as at step 1, we processed the data and narrowed the sample to 2029 enterprises. The results of analyzing the 2029 enterprises data by model2 are shown in Table 9 .

Table 9: The results of the logistic regression analysis of model2

Item	Estimates	Standard Error	ChiSqure	P (Prob>ChiSq)
Whole model test	–	–	296.03	<.0001
Intercept	-1.025	0.244	17.65	<.0001
α' (ln$Email$)	0.267	0.033	66.79	<.0001
β' ($SysV$)	0.023	0.009	6.75	0.009
$\delta 1$ (YY)	-0.395	0.140	7.91	0.005
$\delta 2$ (NY)	-0.107	0.141	0.58	0.446
$\delta 3$ (YN)	-0.194	0.183	1.12	0.289

The model2 is considered significant because the P value of whole model test is less than 0.0001. The fact that (i) the P value of $\delta 1$, the coefficient of variable YY, is less than 0.05 and that (ii) δ_1 has a negative sign implies that continuous adoption of "Defense Measure", "Information Security Policy" and "Human Cultivation" significantly decrease the probability of virus incidents. This result strongly supports our first hypothesis (H1). Another interesting result is that both $\delta 2$ and $\delta 3$, the coefficients of NY and YN, are not significant since their P values are far larger than 0.05. In other words, the second hypothesis (H2) is supported as well;

single period investments without attaching importance to the continuity of adopting security countermeasures make no sense to defence against virus.

4 Conclusions and future works

Through the logistic analysis based on an enterprise survey conducted by the Japanese ministry, we verified that the complementarity of security countermeasures and the continuity of adopting countermeasures have great effects on decreasing the probability of computer virus incidents. In the verification, we took two steps. At the first step, we empirically examined a regression model of IS countermeasures effectiveness based on our former study. The results of this step emphasize the importance of associating "Defense Measures" with "Information Security Policy" and "Human Cultivation". At the second step, we theoretically developed two hypotheses and proved them by our proposed model. It is clearly shown that virus incidents were significantly reduced in the enterprises that took all the three countermeasures both in 2002 and in 2003.

Our approach has a possibility to have further detailed analysis. In fact, since we noted that financial enterprises appear to pay more attention on IS and surfer less virus troubles compared to other enterprises, we put 26 industry dummies into our models to control such industry-dependent characteristics. However, it is not easy to detail what differences of IS investment among the 27-type enterprises. In the future study, we will try to find out how industry characteristics influence security management by grouping respondent enterprises differently or by some other ways.

In the future researches, we might investigate the complementarity of security countermeasures based on another method. Venkatraman examined a general proposition of the performance implications of strategic coalignment [29]. Referring his methodology, we might create a second order construct reflectively measured by its first order constructs in a structural equation modeling and to use the second order construct as a representation of complementarities. Further studies by alternative method would be useful to analyze functions of IS countermeasure complementarity.

Furthermore, we use the data that comes from the survey conducted by METI instead of conducting the survey by ourselves. That is because of the tradeoff between the reliability and the usability of data. METI is a government agency of Japan and their questionnaire is created based on Statistical law, so the official survey data has a high reliability and a large number of samples. On the other hand, the research suffers from the limitation of the data. Since we have to go with the available data, we can not prove our hypotheses by more appropriate methods. As future work, in order to solve the tradeoff, we will launch a project in an attempt to conduct a survey by ourselves and make a deeper examination of IS investment effect by original as well as rich data.

Acknowledgements

The authors would like to make a grateful acknowledgement to the Japan Science and Technology Agency and its Research Institute of Science and Technology for Society (RISTEX) .

This research is supported by Grant-in-Aid for one of the Specified Area Research "Challenges in identifying vulnerabilities hidden in our highly sophisticated information society and exploring solutions" funded by the Japan Science and Technology Agency.

A Appendix

A.1 Industry list:

Manufacturing industries:
1. Manufacture of food, beverage, tobacco and feed
2. Manufacture of textile mill products
3. Manufacture of pulp, paper and paper products
4. Manufacture of chemical and allied products
5. Manufacture of petroleum, coal and plastic products
6. Manufacture of ceramic, stone and clay products
7. Manufacture of iron and steel
8. Manufacture of non-ferrous metals and fabricated metal products
9. Manufacture of general machinery
10. Manufacture of electrical machinery, equipment and supplies
11. Manufacture of information and communication electronics equipment
12. Manufacture of transportation equipment
13. Manufacture of precision instruments and machinery
14. Miscellaneous manufacturing industries

Non-manufacturing industries:
1. Agriculture, forestry, fisheries, cooperative associations and mining
2. Construction
3. Electricity, gas, heat supply and water
4. Video picture, sound information production, broadcasting and communications
5. Newspaper and publishers
6. Information services
7. Transport
8. Wholesale trade
9. Retail trade
10. Finance and insurance
11. Medical and other health services
12. Education and learning support
13. Miscellaneous non-manufacturing industries

References

[1] Michael E. Whitman, 2003. Enemy at the Gate: Threats to Information Security. Communications of the ACM, Vol.46, No.8, August 2003, 91-95.

[2] Anderson, R.j.2001. Why Information Security is Hard: An Economic Perspective. 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, December 10-14th, 2001

[3] Hideyuki Tanaka and Kanta Matsuura,2003. Institutional Design of Information Security Management. Japan Society of Security Management, sponsored by NPO Japan Network Security Association, Network Security Forum 2003, 1-17.

[4] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, 2005. 2005 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. (http://www.gocsi.com/)

[5] Peter Kuper, 2005. The status of Security. IEEE Security & Privacy, 2005, Vol.3, Iss.5, 51-53.

[6] Steve A. Purser, 2004. Improving the ROI of the Security management process. Computers & Security, 2004, Vol.23, 542-546.

[7] Kevin Soo Hoo, 2001. Tangible ROI through Secure Software Engineering. Security Business Quarterly, Vol.1, No.2, Fourth Quarter, 2001. (http://www.sbq.com/sbq/rosi/)

[8] Dr. Daniel E. Geer, Jr., 2001. Making Choices to Show ROI. Security Business Quarterly, Vol.1, No.2, Fourth Quarter, 2001. (http://www.sbq.com/sbq/rosi/)

[9] Lawrence A. Gordon, Martin P. Loeb, 2002. The Economics of Information Security Investment. ACM Transactions on Information and System Security, Vol.5, No.4, November 2002, 438-457.

[10] Hideyuki Tanaka, Kanta Matsuura, Osamu Sudoh, 2005. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. Journal of Accounting and Public Policy, 2005, Vol.24, 37-59.

[11] Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp, Philip H. Enslow, 2005. Assessing Damages of Information Security Incidents and Selecting Control Measures, a Case Study Approach. Workshop on the Economics of Informaition Security 2005.

[12] Itsukazu Nakamura, Toshiyuki Hyodo, Masakazu Soga, Tadanori Mizuno and Masakatsu Nishigaki, 2004. A Practical Approach for Security Measure Selection Problem and Its Availability. IPSJ Transactions, Vol.45, No.8, August 2004, 2022-2033

[13] Sangkyun Kim and Hong Joo Lee, 2005. Cost-Benefit Analysis of Security Investments: Methodology and Case Study. ICCSA 2005, LNCS 3482, 1239-1248.

[14] Bilge Karabacak, Lbrahim Sogukpinar, 2005. ISRAM: information security risk analysis method. Computers & Security, 2005, Vol.24, 147-159.

[15] Scott Dynes, Hans Brechbuhl and M. Eric Johnson, 2005. Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm. Workshop on the Economics of Information Security, 2005 (http://infosecon.net/workshop/schedule.php).

[16] Peter E.D. Lovea, Zahir Iranib, Craig Standinga, Chad Lina and Janice M. Burna, 2005. The enigma of evaluation: benefits, costs and risks of IT in Australian small-medium-sized enterprises. Information & Management, 2005, Vol.42, 947-964.

[17] Erik Brynjolfsson, Lorin M. Hitt, Shinkyu Yang, 2002. Intangible assets: computers and organizational capital. Brookings Papers on Economic Activity, 137-181.

[18] Timothy F.Bresnahan, Erik Brynjolfsson and Lorin M. Hitt. 2002. Information Technology, Workplace Organization, and the Demand for Skilled Labor: Firm-Level Evidence. Quarterly Journal of Economics, Vol.117, Iss.1, 339-376.

[19] Erik Brynjolfsson and Lorin M. Hitt, 2003. Computing Productivity: Firm-Level Evidence. Review of Economics and Statistics, Vol.85, No.4, 793-808.

[20] Hideyuki Tanaka, 2005. A Firm Level Empirical Analysisi of Information Security Investment. 20th Annual Conference of Japan Association for Social Informatics, Kyoto University, Kyoto, September 12-14th, 2005, 185-188.

[21] Ministry of Economy, Trade and Industry. Report on Survey of Actual Condition of IT Usage in 2003. Sep, 2004. http://www.meti.go.jp/policy/consumer/press/0005547/

[22] Amitava Dutta and Kevin McCrohan, 2002. Management's Role in Information Security in a Cyber Economy. California Manage ment Riview, Vol.45, No.1, Fall 2002, 67-87.

[23] Jackie Rees, Subhajyoti Bandyopadhyay, and Eugene H. Spafford, 2003. PFIRES: A Policy Framework for Information Security. Communications of the ACM, Vol.46, No.7, July 2003, 101-106.

[24] Ameet Mallik, Gary S. Pinkus, and Scott Shetter, 2002. Managing Information Security. The McKinsey Quarterly, 2002 Special Edition: Risk and Resilience, 12-15.

[25] Wei Liu, Hideyuki Tanaka and Kanta Matsuura, 2006. Information Security Incidents and Countermeasures :An Empirical Analysis Based on an Enterprise Survey in Japan. 2006 Symposium on Cryptography and Information Security, Hiroshima Prince Hotel, Hiroshima, January 17-20th, 2006.

[26] Hideyuki Tanaka and Kanta Matsuura, 2005. Vulnerability and Effects of Information Security Investment: A Firm Level Empirical Analysis of Japan. The Forum on Financial Systems and Cyber Security: A Public Policy Perspective, College Park, MD, 2005, 1-10.

[27] Atreyi Kankanhalli, Hock-Hai Teo, Bernard C.Y. Tan, Kwok-Kee Wei, 2003. An integrative study of information systems security effectiveness. International Journal of Information Management, 2003, Vol.23, 139-154.

[28] Goodhue,D.L.and Straub,D.W,1991.Security concerns of system users: A study of perceptions of the adequacy of security. Information and Management, Vol.20, No.1, 13-27.

[29] Venkatraman N, 1990. Performance implications of strategic coalignment: a methodological perspective. Journal of Management Studies, Vol.27, No.1, 19-41.