American Journal of Economics and Business Administration 2 (1): 20-26, 2010
ISSN 1945-5488

A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey

Toshihiko Takemura
The Research Institute for Socionetwork Strategies, Kansai University, 3-3-35, Yamate-Cho, Suita, Osaka, Japan, 564-8680

Abstract: Problem statement: The researches in the field of social sciences such as economics and business management were not conducted until around 2000. Particularly, there are few empirical studies on information security. Primary reasons among various ones are that there is no data on information security countermeasures and we cannot easily use the data even if the data exist. Though it is in such a research environment, it is necessary to accumulate the research from not only promotion of academic research but also the social role. In this study, the author quantitatively analyzed Japanese workers' awareness to information security. **Approach:** The author examined whether or not there are differences of the workers' awareness to information security based on various attributes by using Analysis Of Variance (ANOVA) based on non-parametric method. **Results:** It is found that Japanese workers' awareness to information security is different in attributes such as organizational attributes and the education about information security countermeasures. **Conclusion:** The author suggested the necessity of enhancing information security education and introducing firm system such as authority handover system and/or stock option system in order to motivate to take the efficient information security countermeasures.

Key words: Information security, awareness, worker, Analysis Of Variance (ANOVA), web-based survey

INTRODUCTION

It is indisputable that the Internet evolves the individual's life style and the business form in the advanced information society. Especially, by many empirical analyses of Information Technology (IT) it is verified that IT investment contributes to improve not only business performance such as productivity and efficiency, but also GDP and economic growth rate. In other words, by investing in IT asset and introducing IT into business, various positive economic effects are brought. In addition, digitalizing information is promoted in order to use it effectively. In advanced information society many of researchers focused on only such positive economic effects. However, enterprises and individuals are confronted with serious problems. One of them is damage by information security incidents such as illegal access, malware and phishing deal a serious blow to the business. For example, in Japan it is pointed out that compared with the cases of past information leakage, amount of individual and/or secret information run off via the networks becomes enormous (Japan Network Security Association, 2008). To prevent from these damages, many enterprises take various information security countermeasures.

We have much academic researches on information security technology such as cryptographic technology and secured networking in the field of natural science. These accumulated researches achieve a constant result. On the other hand, the researches in the field of social sciences such as economics and business management were not conducted until around 2000. Pioneer and representative researches include theoretical models of information security countermeasures and investment from the viewpoint of economics and management science (Gordon and Loeb, 2002; Varian, 2002). In addition, they discuss the incentive to take information security countermeasures. Hereafter, many researches enhance the above models (Gordon *et al*., 2003; Gordon and Loeb, 2006).

Particularly, there are few empirical studies on information security. Primary reasons among various ones are that there is no data on information security countermeasures and we cannot easily use the data even if the data exist. Therefore, empirical analysis in economics of information security is still in the state of exploratory now at least. It is necessary to accumulate the research from not only promotion of academic

research but also the social role. In Japan, organizations such as Cyber Clean Center, Japan Data Communications Association, Japan Network Security Association and Information-technology Promotion Agency collect and accumulate the data on information security countermeasures and incidents. There are some empirical researches using such data in Japan. For instance, there is an empirical research using data of investigation of actual conditions of processing of information and analyze the information security countermeasures in Japanese firms (Liu *et al*., 2007). Besides this, some researchers accumulate the data by themselves (Takemura, 2009; Takemura and Minetaki, 2009). They use data collected by the survey and analyze effect of the information security countermeasures in Japanese firms. In each research, subjects of these surveys are Japanese firms. Of course, it may be enough to analyze the effect of the information security countermeasures on technologies and management by using aggregated level data such as office and enterprise. Such research have limit because we cannot grasp each worker's awareness to information security, which is important factor. Analyses from the viewpoint of the worker's awareness to information security have appeared (Albrechtsen, 2007; Albrechtsen and Hovden, 2009; Takemura, 2009). Albrechtsen (2007) analyzes the effectiveness of information security countermeasures qualitatively by using data of their interview studies (Albrechtsen, 2007; Albrechtsen and Hovden, 2009). On the other hand, Takemura (2009) analyzes countermeasures by using data collected through Web-based surveys that they conducted themselves (Takemura, 2009). In these researches, it is pointed out that it is meaningless for enterprise to just take the formal countermeasures systematically if the level of awareness to information security is not enough high.

In this study, we analyzes Japanese workers' awareness to information security based on various attributes such as working pattern, organization attributes and individual attributes. Next, we discuss the effective countermeasures through the results of analysis. This result would possess not only academic significance, but also business and political significance.

MATERIALS AND METHODS

Our web-based survey: As mentioned above, at first when we analyze the data on information security countermeasures and investment, we face on scant of the data. In addition, from feature of the research, individual data is needed, but not aggregated data.

Table 1: Arrangement of sample

Working pattern	Listed enterprises	Non-listed enterprises
Regular	200	200
Non-regular	100	100

We analyze the workers' awareness to information security using the data collected through the Web-based survey "investigation on workers' Internet usage and awareness to information security", conducted in March 2009. Subjects of this survey are Japanese people who have been working for more than two years in enterprises. The number of the sample is 600. The sample in this survey is arranged by working pattern and listed/non-listed enterprises as in Table 1.

Table 2 shows basic statistics on indexes of workers' awareness to information security. We investigate awareness to information security by dividing the four kinds of indexes roughly as: (1) recognition concerning individual information, (2) recognition concerning countermeasures and (3) moral awareness of information use. Each index is ordinal scale data and the values are assigned between 1 and 5. The index assigns a small value if the recognition is poor. Inversely, the index assigns a large value if the recognition is rich.

Table 3 shows information on some attributes used as categories. The contents are divided roughly into three kinds of categories: (1) working patterns, (2) organizational attributes and (3) individual attributes. Furthermore, each category has some subcategories.

Hypotheses: From general damage caused by information security incidents, it is clear that the workers' awareness to information security differs according to attributes such as working pattern and organization attributes. Up until now, generally in many surveys, merits of IT usage have been analyzed. However, these merits and awareness to information security have not been quantitatively verified. Therefore, in this study, we examines whether or not the awareness to information security is different by attributes based on the categories in Table 3. He sets up the following hypotheses: (H1) there is no difference in awareness on the information security by working pattern; hypothesis (H2) there is no difference in awareness on the information security by organization attributes and hypothesis (H3) there is no difference in awareness on information security by individual attributes.

Analysis: First, we examines whether hypotheses H1, H2 and H3 are uniform. So, we can examine the level of information security in each group by using median of the groups. Note that a possibility arises such that information security may be kept at a low level even if the awareness of the information security is uniform.

Table 2: The information on indices of workers' awareness of information security

	Variable	Content of questionnaire	Ave.	SD
Recognition concerning individual information	X1	If you can freely see others' individual data such as address, name, age and e-mail address, do you use them?	3.72	0.986
Recognition concerning countermeasures	X21	Do you think that there is a problem using a computer without anti-virus software?	4.12	0.960
	X22	When you receive chain mail, do you think that there might be a problem forwarding the mail to your friends and acquaintances?	4.31	0.911
	X23	Do you think that information security education is not needed if security software has been introduced?	3.70	0.899
	X24	Do you think that information security education is not necessary?	3.91	0.830
	X25	Compared with one year ago, have you changed your attitude to information security, for example, in terms of information management?	3.64	0.632
Moral awareness of information use	X31	Do you think that it is ok to send private mails during work?	3.35	0.941
	X32	Do you think that it is ok to violate any rules if a problem does not occur?	3.78	1.019

Table 3: The Information on attributes (categories)

Category	subcategory	Explanation
Working pattern	Working pattern	1: Regular 2: Non-regular
Organizational attribute	No. of employees	1: Less than 9 persons 2: 10-49 persons 3: 50-99 persons 4: 100-299 persons 5: 300-999 persons 6: 1000-2999 persons 7: 3000-4999 persons 8: 5000-9999 persons 9: 10000-99999 persons 10: 100000-149999 persons 11: More than 150000 persons
	Degree of infrastructure	1: Lowest 2: Low 3: High 4: Highest
	Prohibited matter as information security countermeasures	Taking customer information data outside of the firm by portable devices such as USBs / Attachment of customer information data to e-mail / Taking customer information data outside of the firm by paper/taking a company notebook computer outside the firm / Connecting LAN with private personal computer (1: Overall prohibition 2: Conditional and possible 3: No prohibition)
	Motivational system	Authority handover / Stock option/Employee stock ownership program/Spin-out (1: Introduced 2: Not introduced)
	Listed/non-listed	1: Listed firm 2: Non-listed firm
Individual attributes	Age	1: One's twenties 2: One's thirties 3: One's forties 4: One's fifties 5: One's sixties
	The Internet terms of use	1: Less than one year 2: 1-2 years 3: 2-3 years 4: 4-5 years 5: 6-7 years 6: 8-9 years 7:
More than 10 years	Education about information security	1: Not educated 2: Some formal training and/or the university.

It is important for all workers in society to keep the awareness to information security at high level. Even if many users with a rich awareness of the information security exist, the level of information security in society in general becomes low if even a few users with poor awareness exist. If these hypotheses are verified according to human social factors in addition to quantitative verification, we should be able to reach an understanding of a true security level.

We expect that there will be no difference in awareness of the information security by attributes in the subcategories in Table 3 excluding degree of infrastructure. Takemura *et al*. (2009) have explained forms with a high degree of infrastructure will require higher security levels than in firms with a lower level of infrastructure. Therefore, we expect that there will be a difference in awareness of information security by the degree of infrastructure. And, we can check the level of information security in each group by using the average value and the median of the groups. In order to verify this hypothesis, an Analysis Of Variance (ANOVA) is run.

Before running ANOVA, we need to check whether or not data follows a normal distribution. We have various kinds of tests of normality. Generally, the Kolmogorov-Smirnov test and the Shapiro-Wilk test are accepted as more reliable among various tests. In these tests, the null hypothesis represents data that does not follow a normal distribution. Therefore, if the significance probability is less than 5%, the null hypothesis cannot be rejected and we can conclude that the data do not follow a normal distribution. Oppositely, if the data follows a normal distribution, we can reject the null hypothesis.

Table 4 shows the result of the Kolmogorov-Smirnov test and the Spapiro-Wilk test.

From Table 4, it is found that data in this study does not follow a normal distribution because we cannot reject the null hypothesis. Unfortunately, we cannot run ANOVA by a parametric method such as the t-test and/or Tukey test. Therefore, we should run ANOVA based on a non-parametric method. Concretely, we examine whether or not we have a difference in the median, not in the average, in each category. As a feature of the non-parametric method, data is assumed not to follow the normal distribution and we can use (questionnaire) data with an ordinal scale. Hereafter, we run four kinds of test (ANOVA) according to the categories in Table 3: The Mann-Whitney test, the Wilcoxon test and the Kruskal-Wallis test. Next, we explain briefly the procedure of each test. Refer to (Wasserman, 2007) for details of ANOVA based on a non-parametric method.

First, the Mann-Whitney test (Mann-Whiteney's U test) and the Wilcoxon test are rank sum tests that examine the difference of the median between two groups. In these tests, we use the rank sum of data arranged in ascending order, not the observed data. The test statistics are U and W statistics. Note that we calculate the statistics by using the average rank if there is the same order in data. From these statistics, we calculate the Z-value by using standard deviation and average value. Because the distributions of U and W approximately follow the normal distribution, we can obtain asymptotic significant probabilities from the standard normal distribution table. Incidentally, the null hypothesis in either test is that there is no difference in the median of two groups.

Next, the Kruskal-Wallis test is a rank sum test that examines the difference of the median between more than three groups. Test statistics in this test are calculated by using data arranged in ascending order as well as the Wilcoxon test. We can calculate H statistics and then obtain the asymptotic significant probabilities because the distribution of H statistics approximately follows the chi-square distribution of degree of freedom K-1. Then, we can obtain the asymptotic significant probabilities from the standard normal distribution table because the distributions of these statistics approximately follow the normal distribution. Incidentally, the null hypothesis in either test is that there is no difference in the median of each group (more than three groups).

Table 4: Test of normality

	Kolmogorov-Smirnov test (Search)*		Shapiro-Wilk test	
	Statistics	Significance probability	Statistics	Significance probability
X1	0.204	0.000	0.883	0.000
X21	0.248	0.000	0.807	0.000
X22	0.315	0.000	0.741	0.000
X23	0.285	0.000	0.861	0.000
X24	0.261	0.000	0.851	0.000
X25	0.280	0.000	0.771	0.000
X31	0.212	0.000	0.898	0.000
X32	0.245	0.000	0.866	0.000

*: Modified Lilliefors significance probability

RESULTS AND DISCUSSION

Table 5-20 are results of analysis. From results of analysis, it is found that the workers' awareness to the information security is different by many attributes. In Table 5-20, *, ** and *** represent that p<10%, p<5% and p<1%, respectively.

Table 5: Regular/non-regular

	U	W	Z	Prob.
X1	35464.000	115664.000	-2.369	.018**
X21	38085.500	58185.5000	-1.022	0.307
X22	37618.000	117818.000	-1.318	0.188
X23	39164.500	59264.5000	-0.450	0.653
X24	38112.000	58212.0000	-1.014	0.310
X25	35665.500	55765.5000	-2.412	0.016**
X31	34539.000	114739.000	-2.878	0.004***
X32	37560.000	57660.0000	-1.282	0.200

Table 6: Number of employees

	H statistics	Prob.
X1	10.171	0.426
X21	19.353	0.036**
X22	7.4610	0.681
X23	28.206	0.002***
X24	24.436	0.007***
X25	27.260	0.002***
X31	11.166	0.345
X32	12.557	0.250

DF = 10; Sample size = 600

Table 7: Degree of infrastructure

	H statistics	Prob.
X1	0.8820	0.830
X21	7.0330	0.071*
X22	3.8900	0.274
X23	10.099	0.018**
X24	13.588	0.004***
X25	21.354	0.000***
X31	8.2830	0.041**
X32	12.740	0.005***

DF = 3; Sample size = 600

Table 8: Customer information data taken outside of the firm I

	H statistics	Prob.
X1	5.2180	0.074*
X21	8.6200	0.013***
X22	11.431	0.003***
X23	13.686	0.001***
X24	14.055	0.001***
X25	13.337	0.001***
X31	19.504	0.000***
X32	9.4750	0.009***

DF = 2; Sample size = 526

Table 9: Attachment of customer information data to e-mail

	H statistics	Prob.
X1	9.2650	0.010***
X21	3.0510	0.217
X22	7.2070	0.027**
X23	9.4430	0.009***
X24	10.785	0.005***
X25	18.109	0.000***
X31	25.132	0.000***
X32	8.8002	0.012***

DF = 2; Sample size = 480

Table 10: Customer information data taken outside firm II

	H statistics	Prob.
X1	2.9800	0.225
X21	3.8290	0.147
X22	4.9900	0.083*
X23	11.820	0.003***
X24	12.518	0.002***
X25	16.769	0.000***
X31	16.578	0.000***
X32	6.8380	0.033**

DF = 2; Sample size = 505

Table 11: Taking a notebook computer outside the firm

	H statistics	Prob.
X1	1.7970	0.407
X21	1.9330	0.380
X22	9.8180	0.007***
X23	20.386	0.000***
X24	16.544	0.000***
X25	12.361	0.002***
X31	21.524	0.000***
X32	3.4370	0.179

DF = 2; Sample size = 536

Table 12: Connecting LAN with private personal computer

	H statistics	Prob.
X1	3.9640	0.138
X21	18.866	0.000***
X22	16.762	0.000***
X23	26.487	0.000***
X24	25.681	0.000***
X25	19.483	0.000***
X31	11.742	0.003***
X32	8.3620	0.015**

DF = 2; Sample size = 501

First, as a working pattern, differences in the median of X1, X25 and X31 in Table 5 are at a 1-5% significance level. From the Mann-Whitney test in Table 5 and the statistics in each subcategory, we cannot strictly claim that there is relationship between awareness to information security and regular and non-regular working patterns because the bigness and smallness of the medium is different in each subcategory.

Table 13: Authority handover

	U	W	Z	Prob.
X1	23243.000	147494.000	-1.412	0.158
X21	22525.000	146776.000	-1.925	0.054**
X22	21261.500	145512.500	-2.872	0.004***
X23	22454.500	146705.500	-1.989	0.047**
X24	22577.500	146828.500	-1.902	0.057*
X25	19224.000	143475.000	-4.312	0.000***
X31	25233.500	30486.500	-0.109	0.913
X32	21978.000	146229.000	-2.254	0.024**

Table 14: Stock option

	U	W	Z	Prob.
X1	17242.500	156370.500	-1.501	0.133
X21	14992.000	154120.000	-3.267	0.001***
X22	17099.500	156227.500	-1.704	0.088*
X23	17594.000	156722.000	-1.275	0.202
X24	16477.500	155605.500	-2.137	0.033**
X25	13925.000	153053.000	-4.262	0.000***
X31	16859.000	155987.000	-1.806	0.071*
X32	16128.000	155256.000	-2.354	0.019**

Table 15: Employee stock ownership program

	U	W	Z	Prob.
X1	41087.000	116165.000	-0.066	0.947
X21	37306.000	112384.000	-2.056	0.040**
X22	37548.500	112626.500	-1.999	0.046**
X23	33701.000	108779.000	-3.986	0.000***
X24	34978.500	110056.500	-3.301	0.001***
X25	33944.500	109022.500	-3.986	0.000***
X31	39394.500	114472.500	-0.945	0.344
X32	35443.000	110521.000	-2.987	0.003***

Table 16: Spin-out

	U	W	Z	Prob.
X1	18594.000	156669.000	-0.814	0.416
X21	16979.500	155054.500	-2.061	0.039**
X22	17399.000	155474.000	-1.805	0.071*
X23	17530.000	155605.000	-1.656	0.098*
X24	17925.000	156000.000	-1.350	0.177
X25	14819.500	152894.500	-3.862	0.000***
X31	16253.500	154328.500	-2.579	0.010***
X32	16591.500	154666.500	-2.318	0.020**

Table 17: Listed/non-listed firm

	U	W	Z	Prob.
X1	42968.000	88118.000	-1.001	0.317
X21	41325.500	86475.500	-1.850	0.064*
X22	42662.000	87812.000	-1.220	0.223
X23	40955.500	86105.500	-2.053	0.040**
X24	41180.500	86330.500	-1.935	0.053**
X25	38824.000	83974.000	-3.240	0.001***
X31	40548.000	85698.000	-2.212	0.027**
X32	42635.000	87785.000	-1.171	0.242

Next, in organizational attributes (Table 6-17) we have the differences in the median of many of the subcategories at a 1-10% significance level. Clearly, there are differences in the awareness to information security of workers who belong to organizations that have either some motivational systems or prohibited matter as countermeasures.

Table 18: Age

	H statistics	Prob.
X1	3.279	0.512
X21	0.537	0.970
X22	1.643	0.801
X23	1.609	0.807
X24	10.541	0.032**
X25	2.149	0.708
X31	5.872	0.209
X32	4.268	0.371

DF = 4; Sample size = 600

Table 19: Internet terms of use

	H statistics	Prob.
X1	5.023	0.541
X21	7.293	0.295
X22	8.829	0.183
X23	4.523	0.606
X24	7.522	0.275
X25	4.974	0.547
X31	13.168	0.040**
X32	12.914	0.044**

DF = 6; Sample size = 600

Table 20: Education on information security

	U	W	Z	Prob.
X1	44725.500	83785.500	-0.027	0.979
X21	39309.000	78369.000	-2.761	0.006***
X22	41111.500	80171.500	-1.918	0.055*
X23	32248.500	71308.500	-6.377	0.000***
X24	33323.500	72383.500	-5.817	0.000***
X25	32583.000	71643.000	-6.415	0.000***
X31	42892.000	81952.000	-0.940	0.347
X32	39031.000	78091.000	-2.853	0.004***

From the Mann-Whitney test in Table 13-17 and the statistics in each subcategory, awareness to the information security of workers who belong to organizations with some motivational systems is higher rather than that of workers who belong to organizations without the system. This might imply that the motivational system contributes to improving awareness to information security. In addition, we verify that awareness to the countermeasures of workers in a listed firm is higher than of workers in a non-listed firm. From the Kruskal-Wallis test in Table 6-12 and the statistics in each subcategory, we can only know that the awareness to the information security of workers is different.

Furthermore, as individual attributes (Table 18-20), we have a few differences in the median of subcategories excluding information security and in the educational settings. This implies that education about information security changes the workers' awareness of countermeasures. From the Mann-Whitney test in Table 20 and the statistics in each subcategory, workers who received education on information security have a higher recognition of countermeasures than the other users including self-educated users. Therefore, education in information security is clearly very important.

Finally, we check the three hypotheses. As a result of ANOVA, each hypothesis cannot be affirmed. In order to achieve a higher level of Japanese workers' awareness to information security, we need to discuss countermeasures and strategies in the firm and/or in the government in the future.

CONCLUSION

In this study, we examine whether or not there are differences of Japanese workers' awareness on information security based on various attributes by using ANOVA based on non-parametric method. As a result, it is found that Japanese workers' awareness to information security is different in its attributes such as organizational attributes and the education about information security measures. They experience a difference in awareness in organizations that offer motivation and prohibit certain countermeasures. This implies that their awareness to information security and the countermeasures are affected by the environment of the organization.

The author claims that as some systems to motivate in order to take information security countermeasures we need to enhance to information security education, not just introducing IT tools. This implies that enhancing to information security education would be efficient information security countermeasure in firm.

Researches on the "economics of information security" are not only meaningful in the social sciences, but also essential in real business activities. Therefore, this type of researches needs to accumulate. We will continue to research the social and economic effects of information security countermeasures and investment quantitatively. This will be one of our future endeavors. In this study, we run ANOVA based on non-parametric method, but the information obtained from the results is still not enough as materials for countermeasure examination. By using various social survey methods, we will also continue to research information security countermeasures and investments from the viewpoints of economics and business.

Finally, the author hopes that this study will become an academic contribution to business and economics and will help to give the incentive for firms to invest in and take information security countermeasures.

ACKNOWLEDGEMENT

This research is supported in part by the Ministry of Education, Culture, Sports, Science and Technology, Japan: Grant-in-Aid for Young Scientists (B) (20730196) and the Murata Science Foundation, Japan.

The author is thankful to Hideyuki Tanaka, Kazunori Minetaki, Takuro Imagawa, Makoto Osajima, Atsushi Umino, anonymous referees and some participants at the international conference for helpful comments. Any errors that remain are solely the responsibility of the author.

REFERENCES

Albrechtsen, E., 2007. A qualitative study of users' view on information security. Comput. Secur., 26: 276-289.

Albrechtsen, E. and J. Hovden, 2009. The information security digital divide between information security managers and users. Comput. Secur., 28: 476-490.

Gordon, L.A. and M.P. Loeb, 2002. The economics of information security investment. ACM Trans. Inform. Syst. Secur., 5: 438-457.

Gordon, L.A., M.P. Loeb and W. Lycyshyn, 2003. Sharing information on computer systems security: An economic analysis. J. Account. Pub. Policy, 22: 461-485.

Gordon, L.A. and M.P. Loeb, 2006. Expenditures on Competitor Analysis and Information Security: A Managerial Accounting Perspective. In: Management Accounting in the Digital Economy, Bhimni, A. (Ed.). Oxford University Press, ISBN: 0-19-926038-9, pp: 95-111.

Japan Network Security Association, 2008. Fiscal 2007 Information Security Incident Survey Report (Information Leakage: Projected Damages and Observations). http://www.jnsa.org/en/reports/incident.html

Liu, W., H. Tanaka and K. Matsuura, 2007. Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. Inform. Proc. Soc. Japan Digital Courier, 3: 585-599.

Takemura, T., M. Osajima and M. Kawano, 2009. Economic Analysis on Information Security Countermeasures: The Case of Japanese Internet Service Providers. In: Advanced Technologies, Jayanthakumaran, K. (Ed.). INTEH, ISBN: 978-953-307-009-4, pp: 73-89.

Takemura, T. and K. Minetaki, 2009. The policies for strategic information security countermeasures improving the market value. Proceeding of the 66th Conference on JEPA, (JEPA' 09), Sendai, Japan, pp: 1-19.

Takemura, T., 2009. An economic approach to issues on the information security. RCSS Discussion Paper (Kansai University), 86: 1-21.

Varian, H.R., 2002. System reliability and free riding. ACM Trans. Inform. Syst. Secur., 5: 355-366.

Wasserman, L., 2007. All of Nonparametric Statistics. Springer, ISBN: 978-0387251455, pp: 268.