IPA Information-technology Promotion Agency, Japan

Who Sometimes Violates the Rule of the Organizations?

Empirical Study on Information Security Behaviors and Awareness

Toshihiko Takemura
Kansai University
IPA, Japan

Ayako Komatsu
IPA, Japan

WEIS 2012

Introduction & Background

IPA

- *In this work, we investigate to determine some key factors affecting on employees' behavior of violating the rule related to the information leak*
- Various organizations implement technical or management information security measures, and these measures achieve some positive results
- On the other hand, information security accidents occur even if the organizations implement the measures, and these accidents lead to reduce the (economic) value of the organization

Research Questions

IPA

- With regard to the issue that information security accidents occur even if the organizations implement the measures, we make following hypothesis
  - The organizational measures are one-side measures of managers' standpoints excluding consideration of the employees (users)
  - ➢ This one-side measure may not sometimes work well unless the users understand meaning of the measures
  - ➢ Do employees always comply with the organizational rule ?

IPA

- Current status:
  - Even if the information security policy and organizational rule is established, almost all employees would comply with the rule, but some employees would violate the rule
  - ✓ For instance, in the previous literatures, it is mentioned that *the users might not sometimes comply with the measures or may tend to put dairy-task ahead the measures* even if the policy is established in the organization

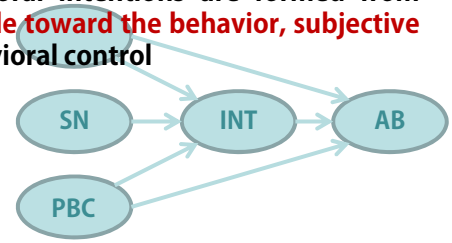
It is a problem

Purpose

- This work focuses on the employee's behavior of violating the rule
- If we can reduce the employees who violate the rule, the organizational measures would be more effective
  - Of course, to some degree, we can prevent to encounter the information security accidents by introducing and operating the information security technologies...

Behavioral modeling

- To tackle the issue on employee's violation of the rule, we build our model into some factors of TPB (Theory of Planned Behavior) widely used in behavioral science
  - TPB shows that the best way to predict an individual's behavior is by examining how that individual intentions to behave
  - In TPB, behavioral intentions influence a certain actual behavior, and the behavioral intentions are formed from three determinants, attitude toward the behavior, subjective norms and perceived behavioral control



- **Logit regression equation**
  - $\ln(p_j/1-p_j) = a + X_b b + X_c c + X_d d + X_e e + X_f f$
    - p_j : the probability that individual violates the rule j
    - X_b : vectors of attitude
    - X_c : vectors of motivation toward the behavior
    - X_d : vectors of awareness
    - X_e : vectors of workplace environment
    - X_f : and the other individual attributes
  - We employ a stepwise procedure for deletion of variables from the model (backward selection procedure)
    - The variables deleted in the selection process are not significant and not affecting factors to the explained variable

Key factors

- **Attitude**
  - Attitude represents the degree to which the individual has a favorable or unfavorable evaluation of the behavior
- **Motivation toward the behavior**
  - Motivation toward the behavior is the driving force by which individual achieves his/her goal
- **Information security awareness**
  - Information security awareness represents the degree to measure individual's evaluation and/or knowledge of the information security
- **Workplace environment**
  - Subjective evaluation regarding the workplace, for example, the degree of workplace satisfaction
  - Objective indicator such as the organizational attribute, for example, the scale of organization

Data Collection

- We use data collected from a Web-based survey entitled "*Survey on Japanese workers' awareness and behavior to information security measures*" which we conducted in March 2011
- This survey includes 1,800 respondents
  - This survey aims at exploring workers' awareness and behaviors to information security measures
  - Subjects of this survey are Japanese people who have been working for more than two years in the same companies
  - The number of survey items is more than 60 including individual attributions such as gender and annual income

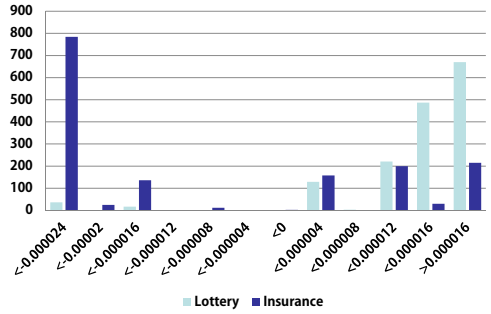
You can access this data set if you contact us

- The behavior of violating the organizational rules (with regard to the information leak)
  1. (Prohibition against) bringing out the secret customer data by using portable devices
  2. (Prohibition against) attaching the secret customer data to e-mail
  3. (Prohibition against) accessing the non-work related website such as 2 Channel at the office -> *non-work related website*
  4. (Prohibition against) forwarding the office's e-mail address to the private address
  5. (Prohibition against) installing the software used at home on office's computer -> *Software piracy*
  6. (Prohibition against) bring out the company's note PC to the outside of company

Cross tabulation between implementation status and individual experiences

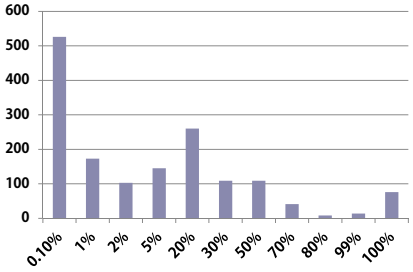
Measures	Status	Individual experiences	
		I have experience	I have no experience
1) Prohibition against bringing out the secret customer data by using portable devices	Totally prohibited	102	685
	Unprohibited	103	160
2) Prohibition against attaching the secret customer data to e-mail	Totally prohibited	55	662
	Unprohibited	93	202
3) Prohibition against accessing the non-work related website	Totally prohibited	56	918
	Unprohibited	165	181
4) Prohibition against forwarding the office's e-mail address to the private address	Totally prohibited	80	578
	Unprohibited	278	237
5) Prohibition against installing the software used at home on office's computer	Totally prohibited	54	854
	Unprohibited	120	180
6) Prohibition against bring out the company's note PC	Totally prohibited	38	501
	Unprohibited	126	162

- **Attitude**
  - Attitude relates mainly to the degree to which the individual has a favorable or unfavorable evaluation of the behavior
  - A positive attitude toward the behavior of violating the rule increases to perform those behaviors
    - The degree of risk aversion (on lottery and insurance) based on BMD method
    - The degree of risk tolerance: the level of risk that individual can perceive, or the degree of loss that they can receive
    - The CFC scale: it is scored so that higher score indicates a greater consideration of future consequences (scoring by factor analysis)
      - The CFC scale used in the field of psychology



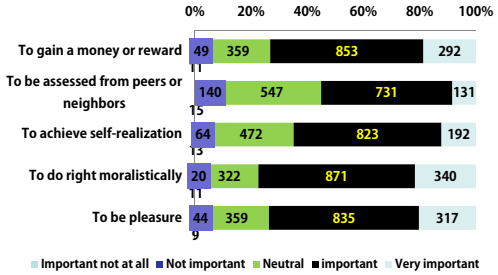
In this article, we assume situations that there is a lottery with a 1% chance of winning 100 thousand JY and a 99% chance of winning nothing, and that there is a 1% chance of being robbed of 100 thousand JY

We ask the following hypothetical question: Now let's assume that your computer at home would be at high risk of becoming infected with computer virus unless you install the latest anti-virus software on the computer. You have the option to purchase and install the latest anti-virus software on your computer or do nothing. Compare the timing (probability of virus infection) in option "A" (implementing the measure) with option "B" (do nothing) and indicate which timing you would prefer to implement the measure for all 10 choice



- **Motivation toward the behavior**
  - In order to measure the motivation, we introduce the importance indicator of five factors with regard to doing something used in the previous study [26]
    - Monetary rewards, assessment from peers, self-realization, morality and pleasantness

In the survey, we directly ask the following question: Now let's assume that you do something. How much importance of the following items



[26] Tsukahara, Y., Human Motivating Behavior and Employee's Behavior. Chida, R., Tsukahara, Y. and Yamamoto, M. (eds), *Behavioral Economics: Theory and Practice*, Tokyo: Keiso-shobo, 50-71, 2010

IPA

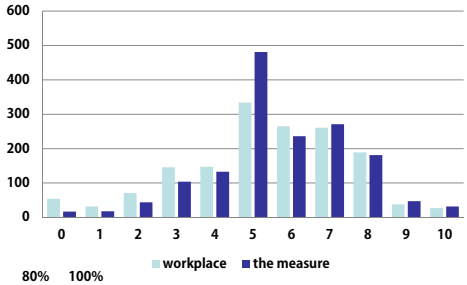
- **Information security awareness**
  - Many previous studies make appeal that it is important to improve the information security awareness and knowledge
  - This survey incorporates 11 questions regarding the information security awareness and the understanding of the measures used in the previous study [35]

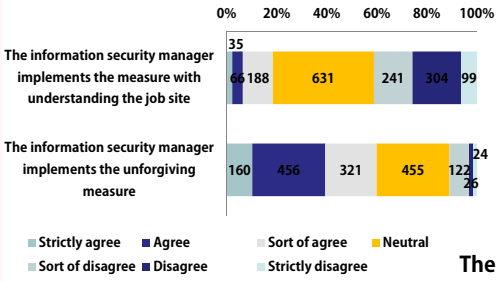
- [35] Takemura, T., A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey. *American Journal of Economics and Business Administration*, Vo.2, No.1, 20-26, 2010

IPA

- **Workplace environment**
  - Workplace environment represents his or her environment surrounding
  - Workplace environment is divided by subjective evaluation regarding the workplace and objective indicator such as the organizational attribute
    - The degree of his or her workplace satisfaction and the organizational information security measure satisfaction
    - The evaluation toward the managers
    - The organizational attributes are listed/non-listed option, the number of employees, and incentive systems for members' working and the employment system which introduced in the organization

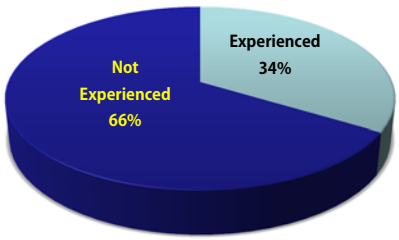
The distributions for the degrees of workplace satisfaction and the measure satisfaction





The evaluations toward the managers

- **The other individual attributes**
  - We have gender, age, education and annual income as popular individual attributes
  - In addition, the experience of encountering the some sort of information security accidents



Estimated Results

- Employing Stepwise (Binary) Logit regression
- We enter 28 explanatory variables, and eventually 8 variables such as "Education" and "Age" are removed in the selection process of either cases

		Coef.	S.E.	z	Remark
1)	Myopic	-0.188	0.110	-1.71	# of obs = 787
	Hypermetro	-0.258	0.113	-2.29	chi2(10) =103.77
	Awareness	-0.320	0.119	-2.69	LL =-251.612
	Satisfaction-WP	-0.079	0.053	-1.50	Pseudo R2 = 0.171
	Manager-2	-0.253	0.085	-2.97	
	Incentive-3	-0.461	0.253	-1.82	
	Employment Sys.	0.573	0.274	2.09	
	Working Pattern	0.948	0.340	2.79	
	Gender	0.523	0.331	1.58	
	Exp. of Accidents	1.119	0.238	4.71	
2)	Myopic	-0.345	0.154	-2.25	# of obs =717
	Hypermetro	-0.307	0.145	-2.11	chi2(10) = 72.31
	Awareness	-0.580	0.149	-3.88	LL = -157.904
	Manager-2	-0.235	0.120	-1.95	Pseudo R2 = 0.186
	Listed	0.501	0.343	1.46	
	Incentive-3	-0.695	0.362	-1.92	
	Employment Sys.	-0.552	0.353	-1.57	
	Working Pattern	0.938	0.425	2.21	
	Income	0.349	0.204	1.71	
	Exp. of Accidents	0.915	0.307	2.98	
3)	Myopic	-0.267	0.141	-1.89	# of obs = 974
	Hypermetro	-0.459	0.142	-3.24	LR chi2(7) = 65.83
	Awareness	-0.490	0.145	-3.37	LL = -181.381
	Manager-1	-0.167	0.106	-1.58	Pseudo R2 =0.154
	Incentive-4	-0.572	0.348	-1.64	
	Working Pattern	0.688	0.343	2.01	
	Exp. of Accidents	0.751	0.295	2.54	
4)	Risk Tolerance	0.065	0.044	1.46	# of obs = 658
	Myopic	-0.319	0.119	-2.67	LR chi2(10) = 69.40
	Hypermetro	-0.219	0.126	-1.74	LL = -208.803
	Motivation-5	0.264	0.171	1.54	Pseudo R2 = 0.143
	Manager-1	-0.296	0.092	-3.22	
	Incentive-2	-0.867	0.469	-1.85	
	Employment Sys.	0.430	0.297	1.45	
	Working Pattern	0.705	0.363	1.94	
	Income	0.274	0.172	1.59	
	Exp. of Accidents	0.863	0.261	3.31	
5)	Myopic	-0.516	0.145	-3.55	# of obs = 908
	Hypermetro	-0.415	0.147	-2.82	LR chi2(8) = 72.74
	Motivation-2	-0.360	0.189	-1.90	LL = -168.392
	Awareness	-0.285	0.144	-1.98	Pseudo R2 = 0.178
	Manager-2	-0.251	0.112	-2.23	
	Incentive-3	-0.635	0.319	-1.99	
	Gender	1.143	0.408	2.80	
	Exp. of Accidents	0.805	0.307	2.62	
6)	Hypermetro	-0.592	0.163	-3.64	# of obs =539
	Motivation-2	-0.623	0.289	-2.16	LR chi2(9) = 61.07
	Motivation-3	0.730	0.312	2.34	LL = -106.874
	Awareness	-0.511	0.166	-3.09	Pseudo R2 = 0.222
	Incentive-1	0.709	0.437	1.62	
	Incentive-2	0.807	0.482	1.68	
	Working Pattern	1.393	0.481	2.90	
	Income	-0.476	0.276	-1.72	
	Exp. of Accidents	0.680	0.381	1.78	

- In all cases, the estimated coefficients of the hypermetro cognition (Hypermetro) and the experience of information security accidents (Exp. of Accidents) are statistically significant in all cases. The former sign is negative and the latter one is positive.
  - Employees who experience the information security accidents tend to violate the rule
- In almost cases, the estimated coefficients of the myopic cognition (Myopic), the information security awareness (Awareness) and working pattern (Working Pattern) are statistically significant, and the sign of the first two coefficients are negative and the sign of the rest is positive.

Concluding Remarks

- From these estimated results, we can find out the some features on the respondent's behavior of violating the organizational rule

1. The individual's attitude toward the risk or the cognition of risk (the psychological factors such as risk aversion and risk tolerance) are not related to the behavior of violating the organizational rule in many cases. On the other hand, both myopic cognition and hypermetro cognition have effects on the behaviors of violating the organizational rules in almost cases.
   - With regard to the behavior of forwarding the e-mail, the more individual can tolerate the risk, the more he tends to violate the rule.
   - the behavior of violating the rule is related to not only the short-term cognition, but also the long-term cognition.

Concluding Remarks

2. The behaviors of violating the rule are related to the motivations on assessment from peers, self-realization and pleasure, not the motivations on the money and morals.
   - Interesting, the greater value on the assessment from peers individual places, the less the tendency to violate the rule is. On the contrary, the individual who places greater value on the self-realization (or pleasure) tends not to comply with the rule.
3. In many cases individual whose information security awareness is higher tends not to violate the rule.
   - The higher the awareness is, the less the tendency to violate the rule is.
4. The behavior of violating the rule is independent of the degree of the measure satisfaction and the number of employees which represents the one scale of the organization, but is not related to the degree of the workplace satisfaction and the evaluation toward the managers in some cases.

Finally...

- It is not easy to control psychological factors such as the individual's attitude toward risk, motivations toward the behaviors or consideration of future consequences.
- Conversely, the factors regard to the organizational attributes such as the degree of workplace satisfaction or the employment system may be controlled by designing the appropriate organizational environment.

Thank you for your attention

Toshihiko Takemura
Kansai University
IPA, Japan
a084034@kansai-u.ac.jp
http://www2.itc.kansai-u.ac.jp/~a084034/