Analysis of Potential Problems in People Management concerning Information Security in Cross–cultural Environment: In the Case of Malaysia

L. Waluyan[1], S. Sasipan[2], S. Noguera[3] and T. Asai[4]

[1]Information Science & Control, Nagaoka University of Technology, Niigata, Japan
[2] Management & Information Systems Engineering, Nagaoka University of Technology, Niigata, Japan
[3] Production Engineering, Simon Bolivar University, Caracas, Venezuela
[4] Management & Information Systems Science, Nagaoka University of Technology, Niigata, Japan
e-mail: asai@kjs.nagaokaut.ac.jp

Abstract

This paper discusses the potential problems due to cultural differences, which foreign companies may face in Malaysia concerning information security. Top five investing countries in Malaysia: Japan, US, Singapore, Germany and UK are examined. Potential problems concerning people management are developed by using Geert Hofstede's and Edward Hall's cultural frameworks. Analyzed are the problems concerning people management. To evaluate the magnitude of potential of problems, a new measure namely Level of Potential (LoP) is adopted. A survey was conducted in Malaysia to evaluate the severity of potential problems and the practicability of LoP. To examine the usability of developed LoPs (logical LoPs), the association level between the logical LoPs and their surveyed LoPs is compared. As a result, LoP can predict problems to a certain extent. The problem "Unintentional sharing of confidential information." is a problem with the highest severity among the potential problems as "teaching others" is encouraged by employees' beliefs.

Keywords

Cultural Differences, Cultural Dimensions, Information Security Management, People Management

1. Introduction

There are still many people who believe that information security management (ISM) is a matter of technology. Nowadays, many incidents such as USB memory losses are reported (Sato and Asai, 2008). Bean (2006) states that 80% of information security breaches are caused by human error. ISM is not only a matter of technology but also a matter of people management. Asai (2007) has pointed out that it is important as well to take people management into account. As people act on their perceptions, which may be influenced by their culture, it is natural to think that culture may have some relations with human errors, especially in cross-cultural environment. However, nobody has carried out a quantitative study on this

relationship yet. Asai and Waluyan (2008) have studied the cultural impact on ISM and measured its magnitude by applying a newly developed measure called Level of Potential (LoP).

The purpose of this paper is to present these potential problems when dealing with information security practices. It also tries to adopt LoP. We conducted a survey in order to evaluate the severity of potential problems and to assure the practicability of LoP. This research may help foreign investors to recognize potential problems due to cultural differences.

We pick up Malaysia because it is considered to be one of the most attractive countries for foreign direct investment. Malaysia is ranked as the fifth most competitive country (WEF, 2008) and as the fifth most favored destination for investment in Asia (The Global Business Policy Council, 2004). Logical analysis of problems and their LoPs will focus on top five investing countries in Malaysia. The top five are Japan (JP), US, Singapore (SG), Germany (DE) and UK. As far as the detailed analysis of severe problems, we adopted the results of survey concerning foreign companies of SG, US and JP only because the data concerning German-based companies and UK-based companies did not have statistically enough number of respondents.

2. Cultural Dimensions

There are extensive theories concerning cultural differences, such as the ones studied by Hofstede (1960), Hall (1976), Trompenaars (2002) and House (2004). We adopt Hofstede's framework of cultural dimension because his study is the most comprehensive concerning how the sense of values in workplaces is influenced by culture and because he analyzed a large database which covered almost all of the major countries (Hofstede, 2002).

Cultural Dimensions	Level	Characteristics
Power Distance Index (PDI)	High	The members expect that some individuals wield larger amounts of power than others.
	Low	Reflects the view that all people should have equal rights.
Individualism (IDV)	High	Ties between individuals are loose.
	Low	Ties between individuals are tight.
Masculinity (MAS)	High	Stress on equity, competition and performance. Managers are expected to be decisive and assertive.
	Low	Stress on equality, solidarity and quality of work life. Managers use intuition and strive for consensus.
Uncertainty Avoidance Index (UAI)	High	Many rules and low tolerance of deviant ideas; resistance to change.
	Low	Few rules and high tolerance of deviant ideas.
Context Culture (CC)	High	**Relationships-centered,** less written.
	Low	**Task-centered,** written.

Table 1: Hofstede's cultural dimensions and context culture

We adopt Hall's context culture as well because it best describes how culture may influence people's preferences in sharing information. Trompenaars is not adopted because his framework focuses on both culture and personality, treating them as the

same, while these two should be treated differently. Finally, the specification of House's framework (2004), which mostly concerns on leadership, has made his framework less applicable to this research. Hofstede's cultural dimensions and Hall's are explained in Table 1. Based on the similarities found between context culture and individualism (IDV) (bold in Table 1), the relationship between high context culture and low IDV, as well as between low context culture and high IDV can be seen.

CD	Degree	Countries						CD	Degree	Countries					
		MY	SG	JP	DE	UK	US			MY	SG	JP	DE	UK	US
PDI	Very low							UAI	Very low		8				
	Low				35	35	40		Low	36				35	46
	Moderate			54					Moderate				65		
	High		74						High						
	Very high	104							Very high			92			
IDV	Very low		20					CC	Very low					√	√
	Low	26							Low				√		
	Moderate			46					Moderate			√			
	High				67				High	√					
	Very high					89	91		Very high		√				
MAS	Very low														
	Low														
	Moderate	50	48												
	High				66	66	62								
	Very high			95											

Table 2: Cultural dimensions (Hofstede) and degrees

To clarify magnitudes of cultural dimensions, each one is divided into 5 degrees, which are very low, low, moderate, high and very high (Asai and Waluyan, 2008). Table 2 shows the classified magnitudes of the cultural dimensions concerned. The countries studied are listed in geographical order. It is found (shown by dotted boxes) that the degrees of UK and US are almost the same. Although Malaysia and Singapore are geographically near, only the score of masculinity (MAS) is quite close to each other. Singapore is close to Malaysia geographically, but not close to it culturally except MAS. UK is far from US geographically, but close to it culturally. Even though two countries are located close, they are not always close culturally.

3. Research Methodology

In order to evaluate the magnitude of potential of problems when a foreign investor applies its own way of business to another country without recognizing the cultural differences or without filling the cultural gaps, this research adopts a new measure, named level of potential (LoP) (Asai and Waluyan, 2008). The LoP is the extent to which problems may arise because of cultural differences. In other words, LoP is the absolute value of the difference between the score of a cultural dimension of an investee country and the respective score of an investor country, see formula (1). To have a detailed categorization, LoP is equally divided into five levels that are very low potential (▲), low potential (△), potential (○), high potential (◎) and very high potential (↓). In this paper, the word "potential" means how soon a problem may become real. It means the probability in other words. The word "severity" means how big influence a problem may cause.

$$LoP = | \, CD \text{ of investor} - CD \text{ of investee} \, |, \qquad \text{...... Formula (1)}$$

where *LoP* = Level of Potential, *CD* = Score of Cultural Dimension.

A set of hypotheses (potential problems, hereafter) was developed based on the results of a pilot survey, which was carried out in November 2007 by interviewing 30 Malaysian employees who were working for foreign companies. Table 3 shows a list of the potential problems and their LoP for each of the studied countries. In this table, the score of overall potential is calculated by accumulating numbers of levels. Numbers 1 through 5 are given to the lowest level (▲) through the highest level (↓), respectively. This table shows that Singaporean companies have the lowest overall potential among the studied countries, while the Japanese have the highest one.

CD	Potential Problems		Countries*				
			JP	US	SG	DE	UK
PDI	Problem 1 Unequal distribution of knowledge about information security policy between managers and subordinates.	LoP	50	64	30	69	69
		State	○	◎	△	◎	◎
IDV	Problem 2 Unintentional sharing of confidential information.	LoP	20	65	6	41	63
	Problem 3 Lower priority to information security policy.	State	△	◎	▲	○	◎
MAS	Problem 3 Lower priority to information security policy. Problem 4 Less reporting or consulting. Problem 5 Difficulty in confirming whether or not Malaysian subordinates. understand an information security policy which has been explained. Problem 6 Possibility of having disgruntled employees.	LoP	45	12	2	16	16
		State	○	▲	▲	▲	▲
UAI	Problem 3 Lower priority to information security policy.	LoP	56	10	28	29	1
		State	○	▲	△	△	▲
Context culture	Problem 7 Getting information too little. Problem 8 Less response to information that is transferred by e-mail.	LoP	20	65	6	41	63
		State	△	◎	▲	○	◎
Overall Potential			26	25	12	22	25

Note: * In order of amount of money invested

Table 3: List of potential problems and their LoP

4.   Analysis of Potential Problems

In order to evaluate the severity of the potential problems and the practicability of LoP, we conducted an Internet-based survey in March 2008. E-mail invitations to our survey were sent to the selected panel members of an Internet research company we hired.

The selected members were Malaysian employees who worked either for Japanese companies, American, Singaporean, German or British in Malaysia. We closed our survey as soon as the number of responses reached our target. People in their twenties and thirties are the largest proportion (92%) of respondents and 55% of them are Malay Malaysians. The Chinese and the Indian are 35% and 5%, respectively. Respondents of these ethnic groups are proportional to Malaysia's demographic. The majority of respondents work in manufacturing (37%) and service sectors (37%), while the rest of them work in education sector (10%) and others (16%). Furthermore, most of them work for Singaporean companies (26%), American (24%) and Japanese (17%).

(March, 2008)

Pro-blems (CD)	Questions	Favorable Answers		Favorable Answers (%)				
		SA/A*	SD/D*	JP N=27	US N=38	SG N=40	DE N=14	UK N=21
P1 (PDI)	**Q1** My boss keeps me educated.		✔	37.0	26.3	15.0	21.4	28.6
	Q2 I carry out my manager's instructions thoroughly.		✔	7.4	7.9	7.5	21.4	9.5
P2 (IDV)	**Q3** I don't mind sharing any skill or knowledge.	✔		96.3	86.8	90.0	92.9	95.2
	Q4 Sometimes. I like sharing anything concerning my job with others.	✔		96.3	92.1	95.0	100.0	95.2
	Q5 Information spreads easily.	✔		74.1	76.3	85.0	100.0	71.4
	Q6 It is better to share any piece of information than keep it to yourself.	✔		92.6	86.8	92.5	100.0	90.5
	Q7 The skills and knowledge that I have acquired personally at work are my valuable assets. Therefore I'm free to use them even after moving to another company.	✔		85.2	76.3	90.0	85.7	81.0
	Q8 According to my morals and values, teaching others with any of my personal experience and knowledge is a good thing to do.	✔		100.0	100.0	100.0	100.0	100.0
P3 (IDV)	**Q9** I hardly decline to help others.	✔		3.7	15.8	32.5	0.0	19.0
	Q10 I place high priority to company's rules above friendship.		✔	55.6	63.2	72.5	42.9	52.4
P3 (UAI)	**Q11** Rules should be flexible.	✔		96.3	94.7	92.5	85.7	90.5
P3 (MAS)	**Q12** Workers should not be burdened with information security-related activities; there should be a specific department to deal with them.	✔		70.4	73.7	82.5	64.3	71.4
P4 (MAS)	**Q13** I don't hesitate to consult my boss about my business activity anytime.		✔	25.9	18.4	15.0	0.0	14.3
P5 (MAS)	**Q14** If I'm asked whether I understand what has been explained or not, I may say "Yes".	✔		59.3	60.5	50.0	42.9	57.1
P6 (MAS)	**Q15** I feel offended if scolded in front of others.	✔		81.5	89.5	75.0	78.6	81.0
	Q16 I'm comfortable with the way my boss warns me.		✔	14.8	13.2	7.5	7.1	9.5
P7 (CC**)	**Q17** My boss gives high priority to face-to-face communications.		✔	14.8	13.2	22.5	14.3	19.0
	Q18 I'm not reluctant to share information even if I'm not asked.		✔	55.6	42.1	35.0	50.0	57.1
P8 (CC**)	**Q19** Face-to-face communications better than e-mail communications.	✔		85.2	84.2	82.5	85.7	85.7

Note: * SA = Strongly Agree, A = Agree, D= Disagree and SD = Strongly disagree   ** CC = Context culture

Table 4: Severities of problems - percentages of favourable answers –

The questionnaire used in the survey was developed to find the magnitudes of the severity of the potential problems when they would take place. Each question has its favorable answer which triggers the associated problem. The higher the percentage of favorable answers is, the higher the severity is. All the questions are listed in Table 4 and their favorable answers are marked by (✔). The results of the survey are also summarized in this table. A problem is considered as serious, if more than 50% of its respondents give favorable answers. To prove which problem is serious, the test on single proportion with 95% level of confidence is adopted. Problems which are serious are marked gray. It can be seen that a half of the potential problems have serious severity if they take place. Four problems (marked gray) concerning IDV, UAI and MAS have serious severity.

4.1. Practicability of LoP

To evaluate the practicability of LoP, a correlation level between LoPs and surveyed severities is calculated. To calculate surveyed severities, a set of the answers is evaluated as the average of weighted answers. The four levels of answers, which are "strongly agree", "agree", "disagree" and "strongly disagree" are weighted with –2, –1, 1 and 2, respectively. The levels of severity can be seen in Figure 1. The coefficients of Pearson's correlation between logical LoPs and surveyed severities are shown in Table 5. Five problems out of eight, have positive medium correlations (see gray marked parts). We can conclude that LoP is practical in proportion to the level of correlation.

Question	LoP	JP	US	SG	DE	UK	Pear. coef*
P1 Unequal distribution of knowledge about information security policy between managers and subordinates.							
1	Severity	-0.2	-0.6	-0.8	-0.6	-0.3	0.35
	LoP	50	64	30	69	69	
2	Severity	-1.1	-1.1	-1.0	-0.8	-0.9	0.52
	LoP	50	64	30	69	69	
P2 Unintentional sharing of confidential information.							
3	Severity	1.2	1.0	1.2	1.3	1.0	-0.75
	LoP	20	65	6	41	63	
4	Severity	1.2	1.2	1.3	1.3	1.1	-0.58
	LoP	20	65	6	41	63	
5	Severity	0.7	0.8	1.0	1.3	0.7	-0.30
	LoP	20	65	6	41	63	
6	Severity	1.2	1.1	1.3	1.4	1.1	-0.52
	LoP	20	65	6	41	63	
7	Severity	0.9	0.9	1.4	1.1	0.8	-0.73
	LoP	20	65	6	41	63	
8	Severity	1.3	1.6	1.5	1.6	1.3	0.14
	LoP	20	65	6	41	63	
P3 Lower priority to information security policy.							
9	Severity	-1.1	-0.7	-0.4	-1.1	-0.7	-0.10
	LoP	20	65	6	41	63	
10	Severity	-0.1	-0.3	-0.5	0.1	-0.0	0.39
	LoP	20	65	6	41	63	

Question	LoP	JP	US	SG	DE	UK	Pear. coef*
11	Severity	1.1	1.2	1.3	1.1	0.9	0.31
	LoP	56	9	28	29	1	
12	Severity	0.5	0.6	0.9	0.3	0.5	-0.37
	LoP	45	12	2	16	16	
P4 Less reporting or consulting.							
13	Severity	-0.6	-0.9	-0.9	-1.3	-0.8	0.58
	LoP	45	12	2	16	16	
P5 Difficulty in confirming whether or not Malaysian subordinates understand an information security policy which has been explained.							
14	Severity	0.3	0.3	0.1	0.1	0.2	0.26
	LoP	45	12	2	16	16	
P6 Possibility of having disgruntled employees.							
15	Severity	0.9	1.1	0.7	0.8	0.8	0.27
	LoP	45	12	2	16	16	
16	Severity	-0.8	-1.0	-1.0	-0.9	-0.7	0.49
	LoP	45	12	2	16	16	
P7 Getting information too little.							
17	Severity	0.8	-0.1	-0.7	-0.8	-0.6	-0.21
	LoP	20	65	6	41	63	
18	Severity	0.1	-0.2	-0.4	-0.1	0.3	**0.44**
	LoP	20	65	6	41	63	
P8 Less response to information that transferred by e-mail.							
19	Severity	0.8	0.9	0.8	0.8	0.8	0.13
	LoP	20	65	6	41	63	

Note: * As to absolute value of coefficient, Weak correlation = 0.1-0.3, Medium correlation = 0.3-0.5, Strong correlation = 0.5-1.0

Table 5: Severity Levels of Pearson's correlation coefficients

Hereafter, 3 problems which have the highest severity among the developed problems are analyzed in depth. This analysis focuses on the problems encountered by Singaporean companies, the American and the Japanese as the majority of the respondents work for these foreign companies. Their number of samples are 40, 38 and 27, respectively. The 3 severest problems that those foreign companies face are outlined in Table 6. To study the relationships between questions and characteristics of respondents, the test of statistical independence with a confidence level of 95% is applied (hereafter, called the test).
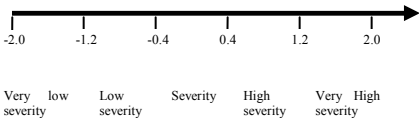

	-2.0	-1.2	-0.4	0.4	1.2	2.0
	Very low severity	Low severity	Severity	High severity	Very High severity	

Figure 1: States of results

Problem		2	3	6	8
Question		8	11	15	19
From		IDV	UAI	MAS	IDV
SG	Severity	1.5	1.3		0.8
	LoP	6	28		6
US	Severity	1.6	1.2	1.1	
	LoP	65	9	12	
JP	Severity	1.3	1.1	0.9	
	LoP	20	56	45	

Table 6: Three most serious problems for each major country

4.2. Singaporean Companies

Problem 2 "Unintentional sharing of confidential information."

There are 6 conditions for Problem 2 (Q3-Q8, Table 5). These 6 conditions **have very high severity** except Q5, the severity of which is 1.0. These facts reveal the reasons of information sharing among Malaysian employees. They are outlined in

order of severity as follows: (hereafter, these names of the categorized reasons are used)

- **Reason 1** *information sharing is morally encouraged* (Q6 and Q8),
- **Reason 2** *the information acquired by their own effort is considered as theirs* (Q7),
- **Reason 3** *information sharing is regarded as natural* (Q3- Q5).

Problem 2 caused by **Reason 2** (Q7) is found to have the highest severity among the selected countries by 0.5, (Table 5). **Reason 2** may cause a direct impact on company's information leakages and this is true, as employees have no conscience about treating confidential information as if it were theirs. Moreover, the result of the test suggests that this reason is dependent on the sector in which respondents work and on their age, (Table 7). It reveals that those who work in manufacturing and service sectors, especially those in their 20's, 30's or 60's are a threat as they have a tendency to share skills and knowledge most.

Concerning **Reason 3,** Q3 is found to be associated with respondents' age, ethnics and religion, as shown in Table 8. It shows that Malaysians in their 40's, especially Indian Malaysians or Hindus, show a low tendency to commit themselves to share information, while the rest of them show a high tendency. Furthermore, as shown in Table 9, it appears that **Reason 3** (Q4) is supported by **Reason 1** (Q6). In other words, Problem 2 is most likely to be caused by their moral standard that "teaching others" is encouraged. Thus information sharing may not be regarded as a breach of security.

		Type of Business *				Age			
		M	S	E	Other	20-29	30-39	40-49	60 or older
(Q7)	Yes	100.0	94.0	50.0	89.0	91.0	94.0	0.0	100.0
	No	0.0	6.0	50.0	11.0	9.0	6.0	100.0	0.0
Total		100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

Note: * M = Manufacturing, S = Services, E = Education.

Table 7: Proportion of answers to Q7 by type of business and age (N=40)

Q5 "Information spreads easily." is the only condition which has high severity, 1.0, lower than the other questions' (Table 5). However, it is the highest among the main selected countries. This may be because information sharing in Japan-based companies and the US-based is not encouraged as much as in Singapore-based companies. Table 5 reveals that five out of 6 conditions (Q3-Q7) for this problem, have the highest severity among the selected countries Singapore's lowest IDV.

(%)		Religion*					Ethnic**				Age			
		I	C	B	H	Others	MY	CH	IM	Others	20-29	30-39	40-49	60 or older
Q3	Yes	95.0	80.0	100.0	0.0	0.0	95.0	88.0	0.0	100.0	95.0	94.0	0.0	0.0
	No	5.0	20.0	0.0	100.0	100.0	5.0	0.0	100.0	0.0	5.0	6.0	100.0	100.0
Total		100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

Note: Hereafter, * I= Islam, C= Christian, B=Buddhism, H= Hinduism,   ** MY= Malay Malaysians, CH=Chinese Malaysians, IM= Indian Malaysians

Table 8: Proportion of answers to Q3 by religion, ethnics and age (N=40)

%		Q4	
		Yes	No
Q6	Yes	94.7	50.0
	No	5.3	50.0
Total		100.0	100.0

Table 9: Proportion of answers to Q6 by Q4 (N=40)

Problem 3   "Lower priority to information security policy."

A tendency to apply rules in a flexible manner is the condition for this problem (Q11). Q11 was asked to know how strict employees apply rules to their activities. A high percentage of favorable answer, 92.5% (Table 4), suggests that a rule is applied in a flexible manner. In general, a rule may not be strictly followed because of employees' personal reasons such as "no time" or "not necessary now". The result of the test reveals that this tendency is associated with respondents' religion and ethnics, as shown in Table 10. It appears that Indian Malaysians or Hindus have this tendency least. Moreover, in comparison with the other two main countries, this tendency is found to have the highest severity, (Q11, Table 5 or 6). One of the reasons for this extreme is probably because of Singapore's UAI, which is "very low" (Table 2).

(%)		Religion					Ethnic			
		I	C	B	H	Others	MY	CH	IM	Others
(Q11)	Yes	100.0	80.0	92.0	0.0	100.0	100.0	94.0	50.0	89.0
	No	0.0	20.0	8.0	100.0	0.0	0.0	6.0	50.0	11.0
Total		100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

Table 10: Proportion of answers to Q11 by religion and ethnics (N=40)

Problem 8   "Less response to information that is transferred by e-mail."

A tendency to respond less to the information transferred by e-mail is probably caused by employees' preference to face-to-face communications, as it is shown by the high percentage of respondents who prefer to direct communications, 82.5%, (Q19, Table 4). This condition may lead to ISM problems, since people ignore e-mail, which may convey important information such as a company's security awareness program.

4.3. American Companies

Problem 2   **"**Unintentional sharing of confidential information."

Similar to Singaporean companies', there are 6 conditions (3 categorized reasons) for Problem 2 although with a different order of severity from Singaporean companies'.

Reason 1 "information sharing is morally encouraged" also turns to be the highest severity among related reasons (Q8, Table 5). However, **Reason 2** (Q7) comes after **Reason 3** (Q3-Q4). This finding implies that the reason of information sharing in the American is most likely to be employees' belief that it is regarded as natural rather than employees' tendency to treat any skill or information as their personal assets. Employees of the American appear to be more conscience-stricken at sharing confidential information. Moreover, a tendency to share any skill and knowledge easily (Q3) is proved to be dependent on respondents' age, religion and ethnics. A similar tendency to Singaporean companies' is seen here.

Problem 3   "Lower priority to information security policy."

A tendency to apply rules in a flexible manner is the condition for this problem. A similar tendency to Singaporean companies' is found. Indian Malaysians show this tendency least. However, the relation between this tendency and respondents' religion was not found.

Problem 6   "Possibility of having disgruntled employees."

A tendency to feel offended in front of others is one of the causes of this problem (Q15). This problem has the highest severity among the selected countries (Q15, Table 5). By comparing the percentage of Singaporean companies with the American who feel comfortable with the way their boss warns them, it appears that Singaporean bosses take a better approach to their subordinates, and that it is higher by 5.7 % (Q16, Table 4).

4.4. Japanese Companies

Problem 2   "Unintentional sharing of confidential information."

Similar to the Singaporean's cases and the American's, there are 6 conditions (3 categorized reasons) that make Problem 2. **Reason 1**, a tendency to share information easily because of their moral standard, is also revealed to be the highest severity among the categorized reasons (Q8, Table 5). Furthermore, similar to Singaporean companies', a tendency to treat any information as if it were theirs (**Reason 2**, Q7) is also found to be associated with a certain age. However, the association between **Reason 2** and business sectors in which respondents' work wasn't found. Moreover, unlike the Singaporean's cases and the American's, age is the only factor which is associated with **Reason 3** (Q3) "information sharing is regarded as natural", where those in their 20's and 30's show the tendency most.

Problem 3   "Lower priority to information security policy."

Unlike the Singaporean's cases and the American's, the test reveals that none of respondents' profiles have a relation with the tendency to treat rules as flexible.

Problem 6   "Possibility of having disgruntled employees."

Similar to American companies' cases, a tendency to feel offended if scolded in front of others (Q15) is the only one accepted condition for this problem. In Japanese companies, it is proved that this tendency is dependent on religion, where Muslim Malaysians and the Christian show this tendency most. The percentage of those who feel comfortable with their bosses' way of warning or scolding is found to be the lowest among the selected countries. This may be because of Japan's MAS, which is "very high" (Table 2).

5.   Conclusions and Future Work

Based on the findings, it is concluded that:

- As for probability, it is logically deduced that Singaporean companies may face problems least because of cultural differences among foreign companies, while Japanese companies face difficulties most.
- As for the practicability of LoP, the results of real survey have shown that LoP can predict the potential of problems to a certain extent.
- As for the severity, the results have revealed that "Unintentional sharing of confidential information." is the problem with the highest severity among the developed problems. This is due to local employees' belief, that is "teaching others" is encouraged. "Lower priority to information security policy." is the second highest because of employees' notion that rules should be flexible. Malaysians have reviewed this paper. Their comments show that these findings are consistent with the characteristics of Malaysian society.

It is hard to generalize the results of survey to a wider population of Malaysia, especially the results related to Indian Malaysians, because of the limitations of the number of samples. To increase the reliability of this study, in the future work, a larger number of samples need to be collected. Moreover, as Hofstede's cultural framework is old and some cultural dimensions change easily as time passes, it is necessary to consider developing a cultural framework which is more dynamic than Hofstede's. His framework is based on the concept that one country has one score for each cultural dimension. This is a weak point when we apply this framework to a multiracial country like Malaysia. It is necessary to verify how far it is applicable. There is another limitation that the results of survey may be contaminated if more than one country invest in a company. To explore threats, vulnerabilities and attacks caused by the explained problems, we shall explain how the potential problems interrelate with components of IT systems by using MSR model.

6.   Recommendations

Within the limitations previously mentioned, this research recommends practical actions to Singaporean companies, American and Japanese. They are summarized in

Table 11. The particulars of respondents' characteristics to which each foreign company should pay attention are also given.

Problems	Recommendations	Pay more attention to		
		SG	US	JP
"Unintentional sharing of confidential information."	1) Convince employees that "teaching others" is not always good in practice of ISM.			
	2) Give employees the right understanding that any skill and knowledge acquired in their companies are not their assets but company's.	Type of business (Manufacturing or service sector) Age (20's and 30's)	-	Age (20's and 30's)
	3) Explain employees that information sharing is a breach of security if it is against Need-to-Know principle	Age (20's and 30's), Religion (except Hindus) Ethnic (except Indian Malaysians)	Age (20's and 30's), Religion (except Hindus), Ethnic (except Indian Malaysians)	Age (20's and 30's)
"Lower priority to information security policy."	4) Give employees the right understanding that a threat to information leakages may attack anytime and anywhere. They have to follow rules without any exception.	Religion (except Hindus) Ethnic (except Indian Malaysians)	Ethnic (except Indian Malaysians)	-
"Less response to information that is transferred by e-mail."	5) Have employees understand that information transferred by e-mail is as important as information that is conveyed directly. 6) Face-to-face communications are the best way to teach them concerning a company's security awareness program.			
"Possibility of having disgruntled employees."	7) Remember that disgruntled employees are a serious threat to information security leakages and their anger may be caused by inappropriate ways of warning.	-		Religion (Muslims, Christians) Ethnic (Malay Malaysians)

Table 11: Recommendations

7. References

Asai, T. (2007), *Information security and business activities,* Kameda Book Services, Niigata, ISBN: 978-4906364589.

Asai, T. and Waluyan, L. (2008), "Potential problems on information security management in cross-cultural environment –a study of cases of foreign companies including Japanese companies in Indonesia –", *Journal of the Japan Society of Security Management,* Vol. 1, No.1, pp15-26.

Bean, M. (2006), *Human error at the center of IT security breach*, http://www.newhorizons. com/elevate/network%20defense%20contributed%20article.pdf, (Accessed 10 February 2008).

Hall, E.T. (1976), *Beyond culture*, Anchor Books, New York, ISBN: 978-0385124744.

Hofstede, G. and Hofstede, G.J. (2004), *Cultures and organizations: software of the mind,* McGraw-Hill, New York, ISBN: 978-0071439596.

House, R.J. (2004), *Culture, leadership, and organizations, the GLOBE study of 62 Societies,* Sage Publications, California, ISBN: 978-0761924012.

The Global Business Policy Council (2004), *FDI Confidence Index*, http://www.atk earney.com/shared_res/pdf/FDICIOct_2004 _S.pdf, (Accessed 5 November 2008).

Sato, S. and Asai, T. (2008), *"Information security management based on baseline approach toward ubiquitous society",* Proceedings of the 41th Conference of Japan Association for Management System, pp170-171.

Straker, D. (2002), *Trompenaars' four diversity cultures*, http://changingminds.org/ explanations/culture/trompenaars_four_cultures.htm, (Accessed 20 September 2008).

WEF (2009), *The global competitiveness report 2008-2009*, http://www.weforum.org/en /initiatives/gcp/Global%20Competitiveness%20Report/index.htm, (Accessed 18 January 2009).