Contemporary Management Research
Pages 117-142, Vol. 7, No. 2, June 2011

Human-Related Problems in Information Security in Thai Cross-Cultural Environments

Tatsuo Asai
Nagaoka University of Technology
E-Mail: asai@kjs.nagaokaut.ac.jp

Suchinthi Fernando
Nagaoka University of Technology
E-Mail: s095191@stn.nagaokaut.ac.jp

ABSTRACT

The purpose of this paper is to discuss potential human-related problems concerning information security, which foreign companies may face in Thailand, and to suggest supplemental countermeasures in international frameworks such as Committee of Sponsoring Organizations of the Treadway Commission and ISO/IEC 27001. These potential problems are predicted using Hofstede's cultural dimensions. To evaluate the magnitudes of potential of problems, a measure named Level of Potential (/LoP/) is adopted. The severity of each problem is calculated based on the results of an empirical survey, which was conducted in Thailand. This paper examines the relations between the conditions of occurrence of problems and the profiles of the respondents. The problem "Using previous company's confidential information" is found to be the severest among all the investor countries considered; the second severest problem is "Unintentional sharing of confidential information" while the problems of "Concealing faults made by friends", "Lower priority to information security management", "Lack of interest in information security management" and "Lack of interest in information outside duties" are also severe. This paper has identified information security management-related problems with their severities and conditions of occurrence for each of the key investor countries in Thailand. It has recommended practical countermeasures to cope with the six serious problems identified.

Keywords: Cultural Differences, Cultural Dimensions, Information Security Management, Human-Related Problems, Thailand

INTRODUCTION

In today’s fast-paced world, success in business is largely dependent on having access to the correct information at the correct time. As Morrill (2006) has pointed out, “The greatest knowledge is to know what intellectual property you own and where it is located on the network”. The moment vital information assets – including trade secrets – are leaked to others, an organization fails to maintain its competitive advantage over others. Thus, securing vital information is of utmost importance to the success of an organization.

In the early days, Information Security was thought of as cryptography and cryptography alone. Whenever any information needed to be secured, enciphering it was the only aspect considered. Yet, Information Security encompasses a lot more than just cryptography. In fact, physical security, network and telecommunications security, operational security, secure development of applications and systems, policies and procedures, access control, laws and ethics, auditing, disaster recovery and business continuity planning are all various areas of information security, which need to be considered along the same lines as cryptography (Harris, 2004). In fact, Asai (2007) has stated that it is important to take human resource security into account as well. The role of information security has now become more management-oriented than technology-oriented. Lacey (2009) defines this as “The shifting focus of information security”. A recent survey stated that 80% of identified information security breaches occur because of human errors (Bean, 2006), and that these errors could occur due to lack of proper knowledge and training, and failure to follow procedures. It is also stated that most people do not feel harmed as long as there is no visible threat. Schneier (2008), in his attempt to understand the psychology of security stated that “Security is both a feeling and a reality”, and that the more our perception of security diverges from the reality, the worse the costs and benefits of security trade-offs are balanced. It is a known fact that a chain is as strong as its weakest link. Since information security has now changed from a technological issue to a behavioural one (Bean, 2006), people – information users – are now identified as the weakest link in the chain of information security. For instance, when considering the process of authentication of a user to a system, the system might check for something the user has (e.g.: token), is (e.g.: biometrics), knows (e.g.: password), or a combination of these (Bishop, 2003). Yet, tokens are stolen or passwords are compromised, more often than not, because of mistakes or slips on the part of the users themselves. They might also reveal other confidential information to other parties who are not authorized to know such information. In business it is important to ensure that access to information is strictly limited to the personnel who need to know it in order to perform their assigned tasks (Schweitzer, 1996). People who need not know a certain piece of information to perform their assigned tasks may not know the value of the information concerned. This could lead to careless handling of information. As a result, important information leaks. Internal Control – Integrated Framework of Committee of Sponsoring Organizations (COSO) (1994) and ISO/IEC 27001 (2005) also emphasize the importance of taking the human factor into consideration when managing information security. These frameworks are international and thus, must contain common, globally usable instructions. So much so, they are not allowed to give practical, local information needed by managers in real business environments. Thus, our paper supplements these documents by providing information regarding the practical aspects which have not been addressed by these documents.

It is stated that people's beliefs and expectations may lead to mistakes, and may cause misjudgements of risks (Pronin, 2006; Komatsu, 2008). Hofstede (2004) states that culture influences people's beliefs and expectations. People from different cultures react in different ways in similar situations. Thus, it can be deduced that mismatches between cultures could lead to unintentional security breaches. Whitfield (2007), states about difficulties faced by foreign managers due to cultural barriers between managers and workers. Cross-cultural environments are, however, growing in importance in today's world of business, which strives for competitiveness through diversity. Diversity is considered a necessary redundancy to enable organizations to cope with unexpected circumstances. Thus, diversity makes even local domestic companies nurture cross-cultural environments.

Empirical qualitative studies on relationships in Information Security Management (ISM) in cross-cultural environments are very limited. Siripukdee, Waluyan, Noguera and Asai (2010) have tried to find out these relationships in Thai companies with foreign management. Thailand was chosen due to its plentiful natural resources and skilled workers, and its wide variety of business areas such as the automotive sector, the electronics and Information and Communication Technology (ICT) sector, etc. (Fdimagazine, 2004).

Asai and Waluyan (2008) have studied the cultural impact on ISM and developed a new measure called the Level of Potential (*LoP*), to measure the probability of occurrence of a problem. Siripukdee, et. al. (2010) have further conducted an empirical survey of Thai subordinates' attitudes related to ISM in foreign companies, to evaluate the practicability of *LoP*. In their survey, the top 8 countries investing in

Thailand were selected by considering the amount of money invested. These countries were Japan, Singapore, US, Hong Kong, UK, Germany, France and Taiwan. Japan being the first on this list, their work was focused on problems faced by Japanese companies in Thailand. Siripukdee, et. al. did not, however, conduct empirical analysis of serious problems which may be faced by the rest of the investor countries. The objective of this paper is to further extend that research into analysing problems faced by these remaining investor countries and to suggest supplemental recommendations to these companies.

ADOPTED CULTURAL DIMENSIONS

Although foreign companies are able to achieve many advantages by investing in Thailand, they would also have to face many problems due to cultural differences between foreign managers – who lack understanding of the local culture – and workers. The COSO (1994) framework also refers to Foreign Operations in Circumstances Demanding Special Attention in Managing Change, where it states: "The expansion or acquisition of foreign operations carries new and often unique risks that management should address. For instance, the control environment is likely to be driven by the culture and customs of local management." This framework refers to corporate culture, whereas, this paper treats national culture, which may influence the former. This paper means the latter by the word "culture".

Extensive theories concerning cultural differences have been presented by the likes of Hofstede (2004), Hall (1976), Trompenaars (Straker, 2002), and House (2004). Hofstede's framework of Cultural Dimensions (CD) concerns how values in the workplace are influenced by culture. Beckmann (2008) states that Hofstede defined "mental programming" or "software of the mind", which is stable over time, making a person react to similar situations in a similar manner. Although Hall noted that ways of communication differ across cultures, he did not present any statistical scores for different countries. Trompenaar's 2x2 model for the diversity of cultures is widely accepted in the business world, but focuses on both culture and personality. House's framework is more focused on leadership across cultures and thus, is not the best suited for this study, which focuses on employees.

Hofstede's scores are based on a comprehensive global survey, and even though many critics argue that assigning a rigid score to a nation is improper – especially among countries with multi-ethnic groups – and that cultural changes over time could make these scores obsolete, studies carried out show that Hostede's dimensions cannot be denied (Beckmann, 2008). In addition, these scores are still being used in researches in many fields of study. Hostede's framework was also adopted by Siripukdee, et. al. (2010) in their research concerning ISM problems in Thai companies. Yates (2006) interpreted Hofstede's cultural dimensions in a concise form as presented in Table 1.

Table 2 presents Hofstede's scores of cultural dimensions for Thailand and the top 8 countries investing in Thailand, listed in geographical order. These scores have been classified into 5 degrees, namely: very low, low, moderate, high and very high, by Siripukdee, et. al. (2010) and by Waluyan, et. al. (2010). As shown by the groupings, the CD of UK and US are almost the same, while Singapore, Hong Kong and Taiwan display similarities concerning PDI, IDV and MAS. This shows that UK and US, although geographically far apart, are culturally close, while Thailand is geographically close to Singapore and Hong Kong, but culturally distant from Singapore concerning UAI and from Hong Kong concerning LTO.

Table 1 Hofstede's Cultural Dimensions

Definition	Level	
	High	Low
PDI (Power Distance Index)	The members expect that some individuals wield larger amounts of power than others.	Reflects the view that all people should have equal rights.
IDV (Individualism)	Ties between individuals are loose.	Ties between individuals are tight.
MAS (Masculinity)	Stress on equity, competition and performance. Managers are expected to be decisive and assertive.	Stress on equality, solidarity and quality of work life. Managers use intuition and strive for consensus.
UAI (Uncertainty Avoidance Index)	Many rules and low tolerance of deviant ideas, resistance to change.	Few rules and high tolerance of deviant ideas.
LTO (Long-Term Orientation)	Persistence, ordering relationships by status, thrift and having a sense of shame.	Personal steadiness and stability, protecting your face, respect for tradition and reciprocation of greeting, favors and gifts.

Source: Yates (2006); Hofstede, G. & Hofstede, G.J. (2004)

Table 2 Hofstede's Cultural Scores Classified by the Degree

Cultural Dimension	Degree	Country								
		TH	SG	HK	TW	JP	DE	FR	UK	US
PDI	Very Low									
	Low						35		35	40
	Moderate	64			58	54				
	High		74	68				68		
	Very High									
IDV	Very Low	20	20		17					
	Low			25						
	Moderate					46				
	High						67	71		
	Very High								89	91
MAS	Very Low									
	Low	34								
	Moderate		48	57	45			43		
	High						66		66	62
	Very High					95				
UAI	Very Low		8						35	
	Low			29						46
	Moderate	64			69		65			
	High							86		
	Very High					92				
LTO	Very Low									
	Low						31	40	25	29
	Moderate	56	48							
	High				87	80				
	Very High			96						

Source: Siripukdee, Waluyan, Noguera and Asai (2010)

RESEARCH METHOD

We assume the real-world business environment where high-level managers dispatched from the home country of the company are not interested in or are not aware of the local culture. Since most problems in such cross-cultural environments occur because of the magnitude of difference of cultural dimensions between foreign managers and local workers – when foreign managers fail to realize the existence of cultural differences or if no effort is made to fill this mind gap –, Asai and Waluyan (2008) proposed a new measure to evaluate this magnitude of potential of problems, named Level of Potential (*LoP*):

LoP = |*CD* of an investor country – *CD* of an invested country *(1)*

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

Thus, they consider *LoP* – the absolute value of the difference between the scores of cultural dimensions of the investor and invested countries – to be the extent to which problems may arise because of cultural differences.

Approach

1. Predict potential problems faced by foreign companies in Thailand based on *LoP*s and the results of a pilot survey carried out. This step was conducted by Siripukdee, et. al.
2. Develop questions by considering conditions, which may trigger the predicted problems. This step was conducted by Siripukdee, et. al.
3. Poll Thai employees working for foreign companies in Thailand. This step was conducted by Siripukdee, et. al.
4. Analyze the collected data to evaluate the severity of problems.
5. Compare actual severity with the predicted potential to test the validity of *LoP*. Since Siripukdee, et. al (2010) have already proved the validity of *LoP*, this step is not demonstrated in this paper.
6. Find problems that may occur, their severities and the conditions which trigger them.
7. Recommend countermeasures to cope with identified triggers and thereby prevent the occurrence of problems.

Hypotheses

Hypotheses (potential problems) were developed by Siripukdee, et. al. (2010) based on the results of a pilot survey concerning employees' attitudes related to ISM. The potential problems and their links to cultural dimensions are presented in Table 3.

Profile of Survey

Table 4 presents the profile of the respondents of the Internet-based survey carried out by Siripukdee, et. al. in March 2008, to evaluate the severity of potential problems and the practicability of *LoP*. It is noted that most respondents were in their 20's and working in manufacturing or service related sectors (Siripukdee, et. al., 2010).

Table 3 Thai Cultural Dimensions and Potential Problems in Thailand

Thai cultural dimensions	Links between cultural dimensions and potential problems *	Potential problems in Thailand	
		No.	Descriptions
Moderate PDI	Less powerful members tend to accept or expect that information (or power) is distributed unequally.	1	Lack of education about the company's ISM.
Very Low IDV	People like to chat with friends while working.	2	Unintentional sharing of confidential information.
	People from birth onwards are integrated into groups, which continue to protect their members in exchange for unquestioning loyalty.	3	Concealing faults made by friends.
	Outstanding attitudes are discouraged by groups.	4	Less reporting or consulting on information security incidents.
		5	Giving less opinions to managers concerning ISM.
Low MAS	People tend to value good working relationship with their managers. They are afraid of problems with their managers.	4 5	Same as above
	High MAS society, such as Japan, is characterized to be assertive and competitive. They are less tolerant of mistakes. High MAS culture would adopt a strong way in scolding subordinates (JETRO,1999). This way may not work well in low MAS society, such as Thailand. If this way is implemented, bad effects may happen unexpectedly (Asai and Waluyan, 2008).	6	Disgruntled employees may come out.
Moderate UAI	In low UAI society, people try to have as few rules as possible. People apply rules to their society flexibly.	7	Lower priority to ISM.
	People in low UAI society don't want to know peripheral information (JETRO,1999). If they decide that information or knowledge related to ISM is not required to their responsibilities, they tend to have less interest in it (Asai and Waluyan, 2008).	8	Lack of interest in ISM.
		9	Lack of interest in information outside duties.
Moderate LTO	People in low LTO society like favors or gifts. They may use previous company's information as a gift.	10	Using previous company's confidential information.

Source: Siripukdee, Waluyan, Noguera and Asai (2010)

The questions used in the survey, to evaluate the ways of thinking of Thai employees and their reactions in response to their foreign managers are listed in Table 5. Each of these questions has its favourable answers, which help the problem to occur. Coloured in grey are the questions for which favourable answers are 'disagree' or 'strongly disagree', whereas, for the other questions, the favourable answers are 'agree' or 'strongly agree'. It is natural to take that the higher the percentage of favourable answer is, the higher the severity is.

Table 4 Characteristics of Respondents

Characteristics		Samples	Percentages
Gender	Male	91	35.7
	Female	164	64.3
Ages	19 or under	4	1.6
	20-29	165	64.7
	30-39	70	27.5
	40-49	13	5.1
	50-59	3	1.2
	60 or older	0	0.0
Types of Business	Manufacturing	107	42.0
	Services	86	33.7
	Education	18	7.1
	Other	44	17.3
Investing Countries *	Japan	81	31.8
	Singapore	17	6.7
	US	66	25.8
	Hong Kong	9	3.5
	UK	34	13.3
	DE	15	5.8
	Other	33	12.9

Source: Siripukdee, Waluyan, Noguera and Asai (2010)

Table 5 List of Questions

Problem	Question	
1	Q1	My manager keeps me educated
	Q2	I apply thoroughly the notice that my manager has shared with me.
2	Q3	I don’t mind to share any skill or knowledge
	Q4	Sometimes, I like sharing anything concerning my job with others
3	Q5	I hardly decline to help others
	Q6	I place high priority to company's rules above friendship.
4	Q7	I don’t hesitate to consult my boss about my business activities anytime
5	Q8	I show my managers any opinion concerning information security management
6	Q9	I can work in any stressful environtment
7	Q10	Rules should be flexible.
	Q11	Before leaving my office, I always make sure everything is kept secure
8	Q12	Information security is a matter of technology
	Q13	I know which information is confidential
	Q14	Workers should not be burdened with information security-related activities, there should be a specific department to deal with that matter
9	Q15	Meetings are held often
	Q16	If I am asked whether I understand the policy or not, I'd rather say "Yes"
10	Q17	The skills and knowledge that I have acquired personnaly at work are my valuable assets. Therefore, I'm free to use them.
	Q18	According to my morals and values, teaching others with any of my personal experience and knowledge is a good thing to do.

Created by the authors based on data by Siripukdee, et. al.

SEVERITY OF POTENTIAL PROBLEMS

The severity of each potential problem and the practicability of *LoP* for Japanese companies were evaluated by Siripukdee, et. al. (2010). Their findings, together with the authors' findings based on the analysis of potential problems for other foreign companies, are presented in this section.

Table 6, summarizes the results of the survey carried out by Siripukdee, et. al. (2010). The average percentage of favourable answers, which exceed 50%, is calculated for each problem. We consider problems for which more than 50% of their respondents gave favourable answers as serious because it implies that most employees tend to make mistakes leading to that problem. These are emboldened. The serious problems are circled. The countries are listed in the order of investment in Thailand. Six out of the ten predicted problems, namely, problems 2, 3, 7, 8, 9 and 10 are found to be serious in foreign companies in Thailand.

Table 6 Severities of Problems According to Percentage of Favourable Answers

From	Problem	Question	JP	SG	US	HK	UK	DE
			n=81	n=17	n=66	n=9	n=34	n=15
Moderate PDI	1	Q1	6.2	11.8	7.6	0.0	11.8	20.0
		Q2	7.4	5.9	0.0	22.2	11.8	13.3
Very Low IDV	②	Q3	**98.8**	**94.1**	**97.0**	**100.0**	**97.1**	**100.0**
		Q4	**90.1**	**88.2**	**93.9**	**88.9**	**91.2**	**80.0**
		Average	**94.4**	**91.2**	**95.5**	**94.4**	**94.1**	**90.0**
	③	Q5	**96.3**	**82.4**	**87.9**	**88.9**	**97.1**	**93.3**
		Q6	**53.1**	**64.7**	**57.6**	**77.8**	**50.0**	40.0
		Average	**74.7**	**73.5**	**72.7**	**83.3**	**73.5**	**93.3**
Very Low IDV & Low MAS	4	Q7	6.2	11.8	27.3	0.0	17.7	13.3
	5	Q8	16.1	0.0	12.1	11.1	32.4	13.3
Low MAS	6	Q9	7.4	17.7	9.1	0.0	14.7	26.7
Moderate UAI	⑦	Q10	**92.6**	**94.1**	**90.9**	**100.0**	**91.2**	**100.0**
		Q11	8.6	5.9	13.6	0.0	11.8	13.3
		Average	**92.6**	**94.1**	**90.9**	**100.0**	**91.2**	**100.0**
	⑧	Q12	**72.8**	**82.4**	**71.2**	**88.9**	**64.7**	**66.7**
		Q13	1.2	11.8	1.5	0.0	2.9	0.0
		Q14	**95.1**	**100.0**	**93.9**	**77.8**	**94.1**	**93.3**
		Average	**84.0**	**91.2**	**82.6**	**83.3**	**79.4**	**80.0**
	⑨	Q15	34.6	29.4	24.2	11.1	26.5	26.7
		Q16	**88.9**	**82.4**	**90.9**	**77.8**	**79.4**	**80.0**
		Average	**88.9**	**82.4**	**90.9**	**77.8**	**79.4**	**80.0**
Moderate LTO	⑩	Q17	**90.1**	**94.1**	**98.5**	**100.0**	**97.1**	**100.0**
		Q18	**98.8**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**
		Average	**94.4**	**97.1**	**99.2**	**100.0**	**98.5**	**100.0**

Created by the authors based on data by Siripukdee, et. al.

SERIOUS PROBLEMS

This section focuses on the problems judged as serious. These are problems 2, 3, 7, 8, 9, and 10 (See Table 6).

Cross-country Analyses

Extensive analyses of the severest problems faced by foreign companies investing in Thailand are presented in this section.

Problem 2: Unintentional Sharing of confidential information.

The questions accepted as conditions for this problem are Q3 and Q4 (see Table 5) (Siripukdee, et. al., 2010).

Q3: “I don’t mind sharing any skill or knowledge.”

Q4: “Sometimes, I like sharing anything concerning my job with others.”

These two conditions show that as employees, sharing information about work may be considered natural in a workplace. This problem has comparably high severity and a high percentage of favourable answers (see Table 6), and can be linked to the fact that Thailand has very low IDV (Siripukdee, et. al., 2010).

Problem 3: Concealing faults made by friends.

Agreeing to Q5 and disagreeing to Q6 are accepted as conditions for problem 3 (see Table 5) (Siripukdee, et. al., 2010).

Q5: “I hardly decline to help others.”

Q6: “I place high priority to company’s rules above friendship.”

This shows that not adhering to rules and failure to follow procedures may be considered as acceptable as long as friendship is safeguarded in the Thai culture.

Problem 7: Lower priority to ISM.

The high percentage of favourable answers in Table 6 shows that this problem, which is triggered by the condition in Q10, has high severity.

Q10: “Rules should be flexible.”

This fact reveals that Thai employees believe that rules are too rigid and difficult to obey and need to be changed as the case may be.

Problem 8: Lack of interest in ISM.

As shown by the high percentages of favourable answers to Q12 and Q14 (see Table 6), which are accepted as conditions for this (see Table 5), this problem has high severity.

Q12: “Information security is a matter of technology.”

Q14: “Workers should not be burdened with information security-related activities. There should be a specific department to deal with that matter.”

This shows that Thai employees may consider ISM a burden, which hampers the progress of their day-to-day work.

Problem 9: Lack of interest in information outside duties.

This problem has high severity as shown by the high percentage of favourable answers to Q16 (see Table 6), which triggers this problem.

Q16: “If I am asked whether I understand the policy or not, I’d rather say ‘Yes’.”

This reveals the fact that Thai employees may pretend to understand the rules laid down by the information security policy even when they truly do not.

Problem 10: Using previous company’s confidential information.

This problem has high severity as shown by the high percentage of favourable answers (see Table 6). Q17 and Q18 are accepted as conditions (see Table 5) (Siripukdee, et. al., 2010).

Q17: “The skills and knowledge that I have acquired personally at work are my valuable assets. Therefore, I’m free to use them.”

Q18: “According to my morals and values, teaching others any of my personal experience and knowledge is a good thing to do.”

This fact reveals that Thai employees may consider the information acquired by themselves as their own – even though it was acquired at another company – and that information sharing is morally encouraged (Siripukdee, et. al., 2010).

These problems are further analysed for each investor country in the next section.

Country-wise Analyses

In order to study the relationships between answers to questions and characteristics of respondents, the test of independence with a 95% level of confidence is applied. Only the cross tables for each pair of variables which show significant correlation to each other are presented here in order of severity of problems.

Japanese Companies

Being the highest in the list of investors, Siripukdee, et. al. (2010), had already examined problems faced by Japanese companies in their study. Thus, only a summary of conclusions made is given here.

- Thai women have a tendency to share information more easily than men.
- A possible contributing factor to hardly declining to help others is lack of experience of information leakage.
- Those with experience abroad tend to place company's rules above friendship.
- Using skills and knowledge acquired at previous companies is dependent on the "Type of business".

Singaporean Companies

Being the second highest investor in Thailand, Singaporean companies are faced with problems 10, 7, 2 and 8 (See Table 6).

Problem 10

While all respondents believed teaching personal experience and knowledge to be good, it is evident from Table 7 that the companies of employees who tend not to consider skills and knowledge acquired at previous companies to be their own free-to-use assets, have previously experienced information leakages.

Table 7 Proportion of answers to Q17 by "Experience of company having suffered information leakages" (N=17)

%		Acquired skills and knowledge are free-to-use assets (Q17)	
		Agree	Disagree
Information leakages	Yes	29.4	5.9
	Unknown	35.3	0.0
	No	29.4	0.0

Problem 7

All respondents working for Singaporean companies agreed that rules should be more flexible. This fact goes on to show that Thai employees in Singaporean companies believe that the rules laid down by their security policies are too rigid.

Problem 2

It can be seen from Tables 8 and 9 that not having a security policy led the employees to not mind sharing skills or knowledge acquired on the job and that most of those who did not like sharing anything concerning the job worked in the Service sector.

Table 8 Proportion of answers to Q3 by "Company has a Security Policy" (N=17)

%		Don't mind sharing skills or knowledge (Q3)	
		Agree	Disagree
Security policy	Yes	82.3	0.0
	Unknown	5.9	0.0
	No	5.9	5.9

Table 9 Proportion of answers to Q4 by "Type of business" (N=17)

%		Like to share anything concerning the job (Q4)	
		Agree	Disagree
Type of business	Manufacturing	23.5	5.9
	Services	47.0	5.9
	Education	5.9	0.0
	Other	11.8	0.0

Problem 8

As shown by Table 10 the companies of most of those who think that information security is not just a matter of technology have enforced security policies. Conversely, Table 11 shows that the companies of most of those who share the same thoughts have either not experienced or are not known to have experienced any information leakages.

Table 10 Proportion of answers to Q12 by "Company has a Security Policy" (N=17)

%		Information Security is a matter of technology (Q12)	
		Agree	Disagree
Security Policy	Yes	52.9	29.4
	Unknown	5.9	0.0
	No	5.9	5.9

Table 11 Proportion of answers to Q12 by "Experience of company having suffered information leakages" (N=17)

%		Information Security is a matter of technology (Q12)	
		Agree	Disagree
Information leakages	Yes	35.3	5.9
	Unknown	11.8	17.6
	No	17.6	11.8

As shown by Table 12, it is interesting to note that the companies of those who do not consider information security-related activities to be a burden are not known to have experienced information leakages.

Table 12 Proportion of answers to Q14 by "Experience of company having suffered information leakages" (N=17)

%		Workers should not be burdened with information security-related activities. There should be a specific department to deal with that matter (Q14)	
		Agree	Disagree
Information leakages	Yes	35.3	0.0
	Unknown	29.4	5.9
	No	29.4	0.0

American Companies

The problems faced by American companies are examined next. These are problems 10, 2, 7 and 9 in order of severity (See Table 6).

Problem 10

In addition to the fact that all respondents agreed that teaching personal experience and knowledge is good, correlation can be found between the answers to Q17 and "Type of business", as shown in Table 13. It is evident from these statistics that the very small percentage of respondents who thought that skills and knowledge acquired at former companies were not their free-to-use asset, belonged to the Service sector. It can also be seen that all respondents thought that teaching personal knowledge and experience is a good thing. Table 14 shows that all respondents who thought acquired knowledge and skills are free-to-use assets also thought that teaching personal experience and knowledge is a good thing to do.

Table 13 Proportion of answers to "Type of business" by Q17 (N=66)

%		Type of Business			
		Manufacturing	Service	Education	Other
Acquired skills and knowledge are free-to-use assets (Q17)	Agree	30.3	41.0	13.6	12.1
	Disagree	0.0	3.0	0.0	0.0

Table 14 Proportion of answers to Q17 by Q18 (N=66)

%		Acquired skills and knowledge are free-to-use assets (Q17)	
		Agree	Disagree
Teaching personal knowledge and experience is good (Q18)	Agree	97.0	3.0
	Disagree	0.0	0.0

Problem 2

Table 15 shows that the answers to Q3 are dependent on "Experience abroad" in such a way that most of the respondents who did not mind sharing skills or knowledge had not had any experience abroad. Thus, it can be deduced that experience abroad would make people rethink before sharing any knowledge or skills acquired on the job. Table 16 shows that most respondents who like to share anything were unaware about whether their companies had suffered any information leakages. Hence, it can be inferred that if a company has suffered information leakages its employees become more cautious about revealing information to others.

Table 15 Proportion of answers to Q3 by "Experience abroad" (N=66)

%		Don't mind sharing skills or knowledge (Q3)	
		Agree	Disagree
Experience abroad	Yes	30.3	1.5
	No	66.7	1.5

Table 16 Proportion of answers to Q4 by "Experience of company having suffered information leakages" (N=66)

%		Like to share anything concerning the job (Q4)	
		Agree	Disagree
Information leakages	Yes	24.2	3.0
	Unknown	37.9	1.5
	No	28.9	4.5

Problem 7

As shown by Table 17, all those who did not consider the rules of the information security policy to be too rigid were females.

Table 17 Proportion of answers to Q10 by “Gender” (N=66)

%		Rules should be flexible (Q10)	
		Agree	Disagree
Gender	Male	36.4	0.0
	Female	60.6	3.0

Problem 9

Table 18 shows that more than half of those who did not pretend to understand the security policy when they truly did not had problems with the management. Conversely, it also shows that most of those who pretended to understand it even when they failed to understand it did not have any problems with the management.

Table 18 Proportion of answers to Q16 by “Experiencing problems with the management” (N=66)

%		If I am asked whether I understand the policy or not, I'd rather say "Yes" (Q16)	
		Agree	Disagree
Problems with management	Yes	25.8	6.1
	No	63.6	4.5

Hong Kong-based Companies

Hong Kong-based companies face problems 7, 10 and 2 (See Table 6), which are examined here.

Problem 7

All respondents working for Hong Kong-based companies agreed that rules should be flexible.

Problem 10

All respondents gave favourable answers to both Q17 and Q18, which lead to problem 10. Table 19 shows that most respondents who believed that acquired skills and knowledge are their own assets and that teaching personal experience and knowledge is good, have not had any experience abroad.

Table 19 Proportion of answers to Q17 and Q18 by “Experience abroad” (N=9)

%		Acquired skills & knowledge are free-to-use assets (Q17)/teaching personal experience & knowledge is good (Q18)	
		Agree	Disagree
Experience abroad	Yes	33.3	0.0
	No	66.7	0.0

Problem 2

Contrary to what is expected, Table 20 shows that the companies of all respondents who did not like sharing anything concerning the job with others did not have a security policy enforced. On the other hand, companies of most of those who like sharing anything had security policies enforced. From this it can probably be inferred that employees fail to understand and adhere to the policy. From the comparison between responses to Q4 and Q16 in Table 21, it can be inferred that employees did not follow the rules laid down by the security policy because they failed to understand them.

Table 20 Proportion of answers to Q4 by "Company has a security policy" (N=9)

%		Like to share anything concerning the job (Q4)	
		Agree	Disagree
Security policy	Yes	77.8	0.0
	No	11.1	11.1

Table 21 Proportion of answers to Q4 by Q16 (N=9)

%		Like to share anything concerning the job (Q4)	
		Agree	Disagree
If I am asked whether I understand the policy or not, I'd rather say "Yes" (Q16)	Agree	88.9	0.0
	Disagree	0.0	11.1

British Companies

UK-based companies are examined next. According to Table 6, these companies are faced with problems 10, 2 and 7.

Problem 10

Table 22 suggests that the answers to Q17 are dependent on "Age" in UK-based companies since all respondents that thought skills and knowledge acquired from a previous company are not their own free-to-use assets were in their 20's. It can also be seen from Table 23 that all respondents who considered teaching personal experience and knowledge to not always be a good thing were females.

Table 22 Proportion of answers to Q17 by "Age" (N=34)

%		Acquired skills and knowledge are free-to-use assets (Q17)	
		Agree	Disagree
Age	20-29	67.6	5.9
	30-39	26.5	0.0

Table 23 Proportion of answers to Q18 by "Gender" (N=34)

%		Teaching personal knowledge and experience is good (Q18)	
		Agree	Disagree
Gender	Male	29.4	0.0
	Female	67.7	2.9

Problem 2

As shown in Table 24, all respondents who minded sharing skills or knowledge belonged to the service sector. Table 25 shows that most respondents who didn't mind sharing skills and knowledge also liked to share anything. On the other hand, all those who didn't like sharing skills or knowledge also didn't like sharing anything concerning the job.

Table 24 Proportion of answers to Q3 by "Type of business" (N=34)

%		Don't mind sharing skills or knowledge (Q3)	
		Agree	Disagree
Type of business	Manufacturing	14.7	0.0
	Service	32.3	5.9
	Education	20.6	0.0
	Other	26.5	0.0

Table 25 Proportion of answers to Q3 by Q4 (N=34)

%		Don't mind sharing skills or knowledge (Q3)	
		Agree	Disagree
Like sharing anything concerning the job with others (Q4)	Agree	85.3	0.0
	Disagree	8.8	5.9

Problem 7

Contradictory to what might be expected, the UK-based companies of all respondents who believed that rules were not too rigid had not experienced any information leakages (see Table 26).

Table 26 Proportion of answers to Q10 by "Experience of company having suffered information leakages" (N=34)

%		Rules should be flexible (Q10)	
		Agree	Disagree
Information leakages	Yes	26.5	0.0
	Unknown	23.5	0.0
	No	44.1	5.9

German Companies

German companies in Thailand face three problems. These are problems 7, 10 and 3 (See Table 6). All respondents from German companies gave favourable answers to Q10 leading to Problem 7 and Q17 and Q18 leading to problem 10, while almost all respondents gave favourable answers to Q5 leading to problem 3.

CONSISTENCY OF FINDINGS WITH OTHERS'

There are not so many studies which refer to Hofstede's cultural framework and information security management at the same time. It is rare to see any study which refers to both of them in cross-cultural environments. Ciganek, A.P. and Francia, G. A. studied the impact of culture on global information security regulations (Ciganek and Francia, 2009). Based on Hofstede's framework, they have remarked that Thailand sits in the opposite side of the United States concerning national culture. The concerned point of ours about the relation between Thailand and the United States is shown in Table 2. Our related results have found that the most serious problem and the second most serious problem are related to long-term orientation and individualism, respectively. These are consistent with their remark. We carried out an international survey, but they did not. In addition, they did not study information security management in cross-cultural environments even though they compared Thai culture with American culture. They showed their comment only based on Hofstede's scores of cultural dimensions. We found potential problems in a more concrete manner based on the surveyed data while they did not.

There are some studies similar to Ciganek and Francia's study. Bjorck and Jiang studied information security and national culture by comparing ERP system security implementations in Singapore and Sweden (Bjorck and Jiang, 2006). They refer to the difference between the cultures concerned, but they do not refer to the difference in cross-cultural environments.

IMPLICATIONS AND RECOMMENDATIONS

The most serious potential problem in foreign companies in Thailand has been found to be “Using previous company’s confidential information.” This implies that we have to classify the knowledge in our office into the skill and the know-how. It is highly recommended to teach them that the former belongs to them and that the latter belongs to their company.

Table 27 Countermeasures for Serious Problems

P#	Serious Problems	Links to CDs	Recommended Countermeasures
2	Unintentional sharing of confidential information	People like to chat with friends while working.	Educate employees about the “Need-to-Know” principle.
			Help employees to understand and obey the security policy of the company.
3	Concealing faults made by friends	People, from birth onwards, are integrated into groups, which continue to protect their members in exchange for unquestioning loyalty.	Teach employees that neither they, nor their friends will be scolded and that it is a good conduct to report any fault.
7	Lower priority to ISM	In low UAI societies, people try to have as few rules as possible. People apply rules to their society’s flexibility.	Employees need to be reminded that ISM is indeed a responsibility of everyone in the company.
8	Lack of interest in ISM	People in low UAI societies do not want to know peripheral information. If they decide that information or knowledge related to ISM is not required to perform their responsibilities, they tend to have less interest in it.	Keep in mind that ISM is not only a matter of technology, but that it also constitutes of a human component.
			Help employees to treat ISM-related activities as a part of their jobs and not feel burdened by these.
9	Lack of interest in information outside duties		Teach employees that everyone is responsible for information security because information leakage gives influence to activities not only in their own department, but also in other departments.
			Try to confirm whether the employees truly understand the enforced security policy by asking them to explain it.
10	Using previous company’s confidential information	People in low LTO societies like favours or gifts. They may use previous company’s information as a gift.	Help employees understand that “teaching others” is not always good in the practice of ISM.
			Help them understand that the know-how or trade secrets are not their own assets, but the company’s.
			Teach employees that it is illegal to use previous company’s know-how or trade secrets.

The second most serious potential problem has been found to be "Unintentional Sharing of confidential information." As Thai people live in high context culture, they chat with each other at work, sharing information even if it is confidential or even if it is not necessary for their colleagues to know for their duties. The managers there need to teach them that any information at work must be managed based on the Need-to-Know principle.

The details of recommendations are summarized in Table 27.

CONCLUSIONS AND FURTHER WORK

Based on the results of the survey carried out by Siripukdee, et. al. on problems of ISM faced by foreign companies investing in Thailand, and from the extended cross-country analysis conducted by the authors, it can be concluded that:

1. The most serious potential problem in foreign companies in Thailand has been found to be "Using previous company's confidential information."
2. The second most serious potential problem has been found to be "Unintentional Sharing of confidential information."

Subsequently, based on the country-wise analysis, it can be concluded that:

1. In Japanese companies, the highest risks of unintentional sharing of confidential information and the use of previous company's confidential information exist in the facts that 98.8% of Thai employees do not mind sharing any skill or knowledge and another 98.8% believe teaching of personal experience and knowledge to be good, respectively.
2. The highest risk of using confidential information of the previous company exists in the fact that 100% of Thai workers in Singaporean companies believe that teaching previous experience and knowledge is good.
3. All Thai workers in American companies think that it is always good to teach personal experience and knowledge, resulting in the highest risk faced by these companies of their employees revealing previous company's information.
4. In Hong Kong-based companies, the highest risks of ISM being given lower priority, and using of previous company's confidential information, exist in the fact that all Thai employees think that ISM rules should be made flexible, in addition to the facts that they consider skills and knowledge acquired at work to be their own assets, and that teaching personal experience and knowledge is good.
5. In British companies, the highest risk of using previous company's confidential information exists in the fact that 100% of Thai employees believe it a good thing

to teach personal experience and knowledge.

6. The two highest risks faced by German companies of lower priority being given to ISM, and of confidential information of the previous company being used, exist in the facts that all Thai employees believe that ISM rules should be made flexible, and consider the skills and knowledge acquired at work as their own assets and that it is good to teach personal experience and knowledge.

Further work of this study shall be carried out in the following areas:

- The occurrence of problems partly depends upon the manager's attitude, since some foreign managers would be interested in studying about the local culture. In this paper, however, we assume the extreme case where managers are unaware of the local culture. Therefore, the warnings listed in this paper are shown under the highest estimation of risk. From the practical viewpoint, we need to look into how much foreign managers are interested in the local culture. Hence, it would be better to expand this study to consider managers as well, instead of limiting it only to workers.
- In order to better understand the situations leading to problems of ISM, it is advised to investigate how national culture influences corporate culture, which seems to be more influential than national culture.

REFERENCES

Asai, T. (2007). *Information security and business activities*. Japan: Kameda Book Services.

Asai, T. and Waluyan, L. (2008). Potential problems in information security management in cross–cultural environment – A study of cases in Indonesia –. *Journal of Japan Society of Security Management*, *21(3)*, 15-26.

Bean, M. (2006). Network defense & product news; Human error at the centre of IT security breach. Retrieved October 9, 2009, from http://www.newhorizons.com/elevate/network%20defense%20contributed%20article.pdf.

Beckmann, D., Menkhoff, L. and Suto, M. (2008). Does culture influence asset managers' views and behaviour? *Journal of Economic Behaviour and Organization*, *67(3-4)*, 624-643.

Bishop, M. (2003). *Computer security: Art and science*. New Jersey: Pearson Education.

Bjork, J. and Jiang, K.W.B. (2006). Information security and national culture comparison between ERP system security implementations in Singapore and Sweden. *Master of Science Thesis for the Royal Institute of Technology,* 1-66.

Ciganek, A.P. and Francia, G. A. (2009). The impact of culture on global information security regulations. Proceedings of the Southern Association for Information Systems Conference, SC, USA, 93-98.

COSO (1994). Internal control – Integrated framework. Retrieved December 28, 2009, from http://www.snai.edu/cn/service/library/book/0-Framework-final.pdf.

Fdimagazine (2004). Invest in Thailand. Retrieved October 20, 2009, from www.fdimagazine.com/news/fullstory.php/aid/797/Invest_in_Thailand.html.

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

Harris, S. (2004). *All in one CISSP certification: Exam study guide (2nd ed.)*. California: McGraw Hill.

Hofstede, G. (2004). Cultural dimensions. Retrieved August 25, 2009, from http://www.geerthofstede.com/hofstede_dimensions.php.

Hofstede, G. and Hofstede, G.J. (2004). *Cultures and organizations: Software of the mind (2nd ed.)*. New York: McGraw-Hill.

House, R.J. (2004). *Culture, leadership, and organizations – The GLOBE study of 62 societies*, London: Sage Publications.

ISO/IEC 27001 (2005). *Information technology – Security techniques – Information security management systems - Requirements,* Geneva: ISO.

Komatsu, A. (2008). Activities of IPA concerning information security and behaviour. *Lecture Notes of the Symposium on Security Psychology and Trust*, 49-62.

Lacey, D. (2009). *Managing the human factor in information security: How to win over staff and influence business*. England: Wiley.

Morril, D. (2006). Disgruntled employees and intellectual property protection. Retrieved October 14, 2009, from http://www.infosecwriters.com/text-resources/pdf/Disgruntled_employees_DMorrill.pdf.

Pronin, E. (2006). Perception and misperception of bias in human judgment. *Journal of Trends in Cognitive Sciences, 11(1),* 37-43.

Schneier, B. (2008). The psychology of security. Retrieved October 9, 2009, from http://www.schneier.com/essay-155.html.

Schweitzer, J. A. (1996). *Protecting Business Information,* Massachusetts: Butterworth-Heinemann.

Siripukdee, S., Waluyan, L., Noguera, S. and Asai, T. (2010). Empirical analysis of human-related problems on information security in cross-cultural environment – Focusing on Japanese companies in Thailand –. *Journal of Information and Management*, *30(4)*, 96-106.

Straker, D. (2002). Trompenaars' four diversity cultures, Retrieved October 9, 2009, from http://changingminds.org/explanations/culture/trompenaars_four_cultures.htm.

Waluyan, L., Blos, M., Noguera, S. and Asai, T. (2010). Potential problems in people management concerning information security in cross-cultural environment – The case of Brazil –. *Journal of Information Processing Society of Japan, 51(2),* 613-623.

Whitfield, G. B. (2007). Business across culture: Equality in the workplace; Retrieved October 9, 2009, from http://www.expat.or.id/business/equality.html.

Yates, M. (2006). Cultural differences, Retrieved February 12, 2008, from http://www.leadervalues.com/content/detail.asp?contentDetaillD-255&Type=More.