1-1-2011

Human-related information security problems faced by British companies in economically rising countries

Suchinthi Fernando
Nagaoka University of Technology, Japan

Tatsuo Asai
Nagaoka University of Technology, Japan

DOI: 10.4225/75/57b52ed1cd8ba
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

HUMAN-RELATED INFORMATION SECURITY PROBLEMS FACED BY BRITISH COMPANIES IN ECONOMICALLY RISING COUNTRIES

Suchinthi Fernando[1], Tatsuo Asai[2]
[1]Graduate School of Information Science & Control Engineering
[2]Department of Management & Information Systems Science
Nagaoka University of Technology
Niigata, Japan
[1]s095191@stn.nagaokaut.ac.jp, [2]asai@kjs.nagaokaut.ac.jp

Abstract

In some cases, global businesses expansion leads to human-related problems due to cultural differences between investor countries and investee countries. This study focuses on such problems in the area of information security. Potential problems which British companies may face in rising economies are discussed here. Russia, India and China, where UK is one of the key investors, are examined. Potential problems were developed by using Hofstede's framework of culture and the recently proposed theory of Level of Potential (LoP) was adopted to predict their magnitudes. Three online surveys were conducted in Russia, India and China to evaluate the severity of the potential problems and the practicability of LoP. It is proved that the theory of LoP can predict problems for British companies in economically rising business environments to a certain extent. The results reveal that the problem of "Unintentional sharing of confidential information" has the highest severity in Russia and India, while the problem of "Using any means to reach goals owing to high competition" has the highest severity in China.

Keywords

Information security management, human-related problem, cultural dimension, cultural difference, level of potential, the UK, Russia, India, China

INTRODUCTION

The fast growing developing economies of Russia, India and China, three of the four economically rising countries commonly referred to as BRICs for Brazil, Russia, India and China, where UK is one of the key investors, are forecasted to be within the top 5 most attractive destinations for foreign direct investment (FDI) during the time span of 2010-2012. According to United Nations' World Investment Prospects Survey 2010-2012 (United Nations, 2010) China, India and Russia are ranked 1st, 2nd and 5th most favoured FDI destinations, respectively. Yet, in order to achieve the benefits offered by investing in these countries, high-ranking officials dispatched from the company's home country should be aware of the local culture. Internal Control – Integrated Framework of Committee of Sponsoring Organizations (COSO) 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" (COSO, 1994). This framework seems to refer to corporate culture, whereas this paper treats national culture, which may influence the former. Whitfield (1997) studies the difficulties faced by foreign managers due to cultural barriers between their local workers and themselves.

Inadvertently, these cultural differences impact information security as well. Although information security focused mainly on technological aspects in the early days (Harris, 2004), Asai (2007), the COSO framework (1994) and ISO/IEC 27001 (2005) emphasize the importance of taking human resource security into consideration when managing information security. Bean (2008) states that most identified information security breaches occur because of human errors resulting from lack of proper knowledge and training, and failure to follow procedures. Lacey (2009) defines this change in the role of information security from being technology-oriented to more management-oriented as "the shifting focus of information security". In order to succeed in business, however, 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). According to Pronin (2006), people's beliefs and expectations may lead to mistakes and misjudgements of risks. Hofstede, G. and Hofstede,

G. J. (2004) show how people's beliefs and expectations are influenced by their culture. Hence, it can be inferred that mismatches in cultures between management and employees could lead to unintentional security breaches.

Studies on relationships in Information Security Management (ISM) in cross-cultural environments were very limited until recently, when a new theory named Level of Potential (*LoP*) was developed to measure the magnitude of cultural impacts on ISM (Asai & Waluyan, 2008). UK being within the top 6 investors of each of Russia (RU), India (IN) and China (CN), this paper explores potential human-related problems in information security, which could be faced by British companies in these countries because of cultural differences between the local employees and the management dispatched from UK.

CULTURAL DIMENSIONS

Although being able to achieve many advantages by investing in economically rising countries, foreign managers who fail to understand cultural differences would also have to face problems in information security. Extensive theories have been presented by the likes of Hofstede, G. and Hofstede, G. J. (2004), Hall (1976), Trompenaars (Straker, 2002), and House, Hanges, Javidan, Dorfman and Gupta (2004) concerning cultural differences. Of these, we use Hofstede's framework of Cultural Dimensions (CD) for this study as it concerns how values in the workplace are influenced by culture (Hofstede, G & Hofstede, G. J., 2004) and provides numerical scores.

The scores for CDs measured by Hofstede are based on a comprehensive global survey and have been able to withstand many criticisms and are still being widely used in many researches in many fields of study (Beckmann, Menkhoff & Suto, 2007). These CDs are summarized by Yates (2006) as presented in Table 1.

Table 1: Hofstede's Cultural Dimensions (Yates, 2006)

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, favours & gifts.

Table 2 presents Hofstede's scores for UK, Russia, India and China. These scores have been classified into 5 degrees, namely: very low, low, moderate, high and very high by equally dividing the range of scores between the highest score and the lowest score for each CD among the scores of all countries (Asai & Waluyan, 2008). It should be noted that no score of LTO is given to Russia, and thus, no calculation concerning LTO is carried out concerning Russia. Figure 1 represents Hofstede's cultural scores for each of these countries graphically. The groupings of Table 2 marked by broken lines and coloured grey, and Figure 1 imply that British companies may have less MAS-based problems in China, and less UAI-based problems in India and China. The correlation matrix of cultural scores in Table 3 shows that India and China have some similarity in their cultural aspects, while Russia differs somewhat. It also shows that UK stands culturally apart from the investee countries.

Table 2: Hofstede's Cultural Scores Classified by the Degree

Cultural Dimension	Degree	Country			
		UK	RU	IN	CN
PDI	Very low				
	Low	35			
	Moderate				
	High			77	80
	Very high		93		
IDV	Very low				20
	Low		39		
	Moderate			48	
	High				
	Very high	89			
MAS	Very low				
	Low		36		
	Moderate			56	
	High	66			66
	Very high				
UAI	Very low				
	Low	35		40	30
	Moderate				
	High				
	Very high		95		
LTO	Very low				
	Low	25			
	Moderate			61	
	High				
	Very high				118

[a] RU: Russia, IN: India, CN: China (ISO country codes)

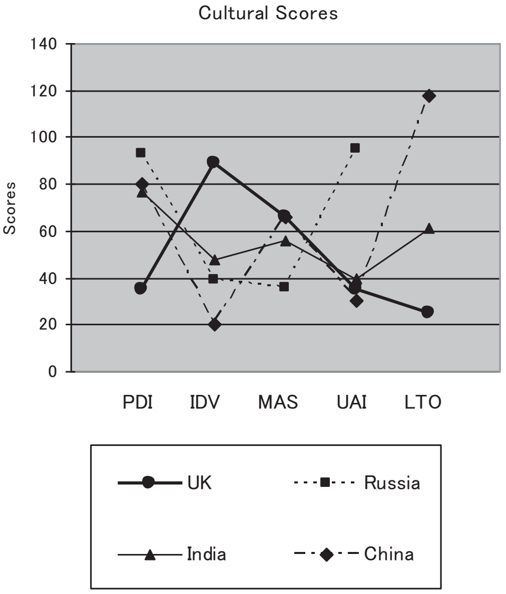

Figure 1: Hofstede's Cultural Scores

Table 3: Correlation Matrix of Hofstede's Cultural Scores

	UK	RU	IN	CN
UK	1.00			
RU	-0.92	1.00		
IN	-0.34	0.20	1.00	
CN	-0.65	0.20	0.68	1.00

RESEARCH METHOD

Assumption

In this study it is assumed that most problems in effectively implementing security policies in cross-cultural environments occur because of the differences in culture between foreign managers and local workers, when foreign managers fail to realize the existence of cultural differences or fail to understand these differences.

Level of Potential

It has been proved that the likelihood of occurrence of problems is correlated to the magnitude of difference of cultural dimensions between investor and investee countries and a new measure named Level of Potential (*LoP*) was proposed to evaluate this magnitude of potential of problems (Asai & Waluyan, 2008), where *LoP* is calculated as in Equation (1).

$$LoP = |CD \text{ of an investor country} - CD \text{ of an investee country}| \quad \cdots\cdots (1)$$

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

Thus, *LoP*, the absolute value of the difference between the scores of cultural dimensions of an investor country and an investee country, is considered to be the extent to which problems may arise because of cultural differences. In this research *LoP* is used to predict potential problems, which may be faced by British companies investing in Russia, India and China.

Approach

We develop practical potential problems, utilizing real business experiences and Hofstede's scores of the related countries. Comparing the results of a survey concerning local employees' reactions with logical predictions by the theory of *LoP* enables us to evaluate the appropriateness of this theory. Until its practicability is proved, we should keep this comparison. We believe that it is natural to follow the steps listed below:

Predict potential problems in each of the investee countries based on *LoP*s, the results of pilot surveys carried out, the authors' experience of working for foreign companies, and based on the experiences gained through surveys previously conducted in other countries with similar cultural scores.

(1) Develop questions by considering conditions, which may trigger the predicted problems.
(2) Poll Russian, Indian and Chinese employees working for foreign companies.
(3) Analyze the collected data to evaluate the severity of problems.
(4) Compare the actual severity with the predicted potential to test the validity of *LoP*. Since the validity of *LoP* has already been proved (Waluyan, Blos, Noguera & Asai, 2010), this step is not demonstrated in this paper.
(5) Find the problems that may occur and the conditions which trigger them.
(6) Recommend countermeasures to cope with identified triggers and thereby prevent the occurrence of problems.

POTENTIAL PROBLEMS FACED BY BRITISH COMPANIES

Three separate studies concerning top investor countries in each of these economically rising countries were conducted in 2010, where the *LoP*s between the investee country and its top investor countries were calculated. The *LoP*s between UK and each of these countries are shown in Table 4. The areas which could lead to problems are identified by equally dividing the *LoP* for a particular CD into 5 classes, from very low to very high potential (Asai & Waluyan, 2008). The areas with potentials, except very low potential, are coloured grey.

Table 4: Level of Potential (LoP)

	RU	IN	CN
PDI	58	45	45
IDV	50	41	69
MAS	30	10	0
UAI	60	5	5
LTO	–	36	93

It can be predicted from these calculations that British companies may face problems based on PDI and IDV in all three of these countries, while they may face MAS- and UAI-based problems in Russia. They may also experience some problems in India and China due to differences in LTO between UK and these countries.

In these three studies, Internet-based surveys were conducted by our creating and hosting questionnaires supported by the Survey Monkey Online Survey Software and Questionnaire Tool. The services of AIP Corporation, Marketing Research Division, were employed to administer the surveys in Russia, India and China. AIP Corporation has panels consisting of members ready to respond to such surveys. The screening questions included at the beginning of the questionnaire ensured that only Russian, Indian and Chinese nationals working for foreign companies in Russia, India and China, respectively, were allowed to proceed with the rest of the questions in the survey. The screening questions also ensured that only workers or low-level managers under foreign high-level managers responded to the survey, by screening out directors and higher-level managers. These respondents responded to these surveys through user accounts created by AIP Corporation to make access to our questionnaires hosted on the Survey Monkey System.

Problems in Russia

Potential problems were developed based on experience gathered through previous surveys conducted in countries with similar cultural scores as Russia and the results of a pilot survey carried out by interviewing

Russians concerning employees' attitudes towards ISM (Asai, Fernando & Castillo, 2011). These potential problems, the relevant cultural dimensions and their links are presented in Table 5. The characteristics of the 152 Russian respondents of the survey carried out in June 2010 are presented in Table 6. These respondents were Russian nationals working for Dutch, British, German, American or Japanese companies in Russia. Of these, the responses by the 34 respondents working for British companies were used for this study. Most respondents were male, in their 30's and working in the service-related or manufacturing sectors. Table 7 summarizes the results of this survey. The column titled "Original Problem Number" in this table refers to the number given to the problems in each of these separately conducted studies, whereas the column titled "New Problem Number" refers to the problem number given to that same problem in the newly compiled list containing all the problems considered in these three separate studies (see Table 14). This helps in identifying the new number to which the problem is converted in this comparative study. The questions used in this survey are available in Reference (Asai, Fernando & Castillo, 2011). Each of these questions has a set of answers which help the problem to occur. It is natural to take that the higher the percentage of problem-causing answers is, the higher the severity is. Problems for which more than 50% of their respondents gave problem-causing answers are considered as serious because it implies that most employees tend to make mistakes leading to that problem. These are emboldened, while the numbers of the serious problems are circled. According to Table 7 it can be seen that P4 "Unintentional sharing of confidential information" is the severest problem in Russia, while P5 "Concealing faults made by friends" and P10 "Unwilling to follow information security policy without complete understanding" also have high severity.

Table 5: Russian Cultural Dimensions and Potential Problems in Russia (Asai, Fernando & Castillo, 2011)

Russian Culture	Link[a]	P#	Problem
Very High PDI	People accept that power and wealth is normally distributed unequally within the society.	1	Unequal distribution of knowledge on company's ISM
Low IDV	People like to work in groups. People like to chat with friends while working. Friendship is highly valued. Relationship-centred society.	2	Unintentional sharing of confidential information
		3	Concealing faults made by friends
		4	Less task-centred and more oriented to chat with co-
Low MAS	Get involved in activities which are considered less masculine. Value good relationship with managers.	5	Less reporting or consulting on ISM incidents.
		6	Not giving opinions to managers concerning ISM.
		7	Disgruntled employees.
Very High UAI	Not open to unstructured ideas and situations. Society may follow rules laid down to control unexpected situations only after fully understanding them.	8	Unwilling to follow information security policy without complete understanding.

[a] Expressions used for links are picked up from Hofstede, G. and Hofstede, G. J. (2004)

Table 6: Characteristics of Russian Respondents (Asai, Fernando & Castillo, 2011)

Age:	
Below 20	1
20-29	65
30-39	72
40-49	12
50-59	2
60 or older	0
Sex[a]:	
Male	97
Female	43
Type of business[b]:	
Manufacturing	66
Services	67
Education	3
Other	15
Experience abroad:	
Yes	91
No	61

[a] 12 respondents refrained from answering this question
[b] 1 respondent refrained from answering this question

Table 7: Severities of Problems in Russia According to Percentage of Problem-Causing Answers (Asai, Fernando & Castillo, 2011)

(n=152)

CD	Original Problem Number	New Problem Number	Overall Severity (%)
PDI	1	P1	14.7
IDV	②	P4	**94.1**
	③	P5	**52.9**
	4	P6	35.3
MAS	5	P3	20.6
	6	P2	35.3
	7	P7	32.4
UAI	⑧	P10	**52.9**

Problems in India

Potential problems were developed based on the degrees of Indian cultural dimensions shown in Table 2, the authors' experience in working for foreign companies and the results of a pilot survey conducted by interviewing Indians concerning employees' attitudes related to ISM (Fernando, Das & Asai, 2010). These potential problems, the relevant cultural dimensions and their links are presented in Table 8, while Table 9 presents the characteristics of the 151 respondents of the survey carried out in February 2010. These respondents were Indian nationals working for Singaporean, American, British, Dutch or Japanese companies in India. Of these, the responses by the 30 respondents working for British companies were used for this study. Most respondents were in their 20's, male and working in the information technology industry or service-related sectors. Table 10 summarizes the results of this survey. The questions used in this survey are available in Reference (Asai & Fernando, 2010). Table 10 shows us that P4 "Unintentional sharing of confidential information" is the severest problem for British companies in India, followed by P9 "Less interest in ISM", P5 "Concealing faults made by friends", P14 "Using previous company's confidential information", P2 "Not giving opinions to managers concerning ISM" and P8 "Using any means to reach goals owing to high competition".

Table 8: Indian Cultural Dimensions and Potential Problems in India (Asai & Fernando, 2010)

Indian Culture	Link[a]	P#	Problem
High PDI	Less powerful members tend to accept or expect that information (or power) is distributed unequally.	1	Unequal distribution of knowledge on company's ISM
		2	Not giving opinions to managers concerning ISM
		3	Less consulting or reporting on ISM incidents
Moderate IDV	People like to work in groups. Friendship is highly valued. Relationship-centred society.	4	Unintentional sharing of confidential information
		5	Concealing faults made by friends
Moderate MAS	Get involved in activities which are considered less masculine. Value good relationship with managers.	6	Using any means to reach goals owing to high competition
Low UAI	More open to unstructured ideas and situations. Society may not follow rules laid down to control unexpected situations.	7	Less interest in ISM
Moderate LTO	Favours gifts (previous company's information could be used as a gift).	8	Using previous company's confidential information

[a] Expressions used for links are picked up from Hofstede, G. and Hofstede, G. J. (2004)

Table 9: Characteristics of Indian Respondents (Asai & Fernando, 2010)

Age:	
Below 20	8
20-29	103
30-39	25
40-49	11
50-59	3
60 or older	1
Sex[a]:	
Male	113
Female	36
Type of business:	
IT	56
Manufacturing	22
Services	43
Education	18
Other	12
Experience abroad:	
Yes	57
No	94

[a] 2 respondents refrained from answering this question

Table 10: Severities of Problems in India According to Percentage of Problem-Causing Answers (Asai & Fernando, 2010)

(n=151)

CD	Original Problem Number	New Problem Number	Overall Severity %
PDI	1	P1	13.3
	②	P2	**66.7**
	3	P3	33.3
IDV	④	P4	**90.0**
	⑤	P5	**76.7**
MAS	⑥	P8	**53.3**
UAI	⑦	P9	**83.3**
LTO	⑧	P14	**73.3**

Problems in China

Potential problems were developed by Asai, Qin and Caibutengdaoriji (2011) based on previous experience gained through surveys conducted in countries with similar cultural scores as China and the results of a pilot survey conducted by interviewing Chinese employees working for foreign companies. These potential problems, the relevant cultural dimensions and their links are presented in Table 11, while Table 12 presents the characteristics of the 186 Chinese respondents of the survey carried out in May 2010. These respondents were Chinese nationals working for Taiwanese, American, Japanese, Korean, Singaporean or British companies in China. Of these, the responses by the 30 respondents working for British companies were used for this study. It is noted that most respondents were in their 30's and working in the manufacturing sector. The questions used in this survey are available in Reference (Asai, Qin and Caibutengdaoriji, 2011). Table 13 summarizes the results of this survey and shows that all of the eight predicted problems have high severity for British companies in China with P8 "Using any means to reach goals owing to high competition" being the severest, followed by P1 "Unequal distribution of knowledge on company's ISM" and P11 "Lower priority to information security policy". P14 "Using previous company's confidential information" is the next severest problem, followed by P4 "Unintentional sharing of confidential information", P5 "Concealing faults made by friends" and P12 "Receiving too little information", while P13 "Sharing of information depends on the relationship rather than the principle of need-to-know" also has high severity.

Table 11: Chinese Cultural Dimensions and Potential Problems in China

Chinese Culture	Link[a]	P#	Problem
High PDI	Less powerful members tend to accept or expect that information (or power) is distributed unequally.	1	Unequal distribution of knowledge on company's ISM
Very Low IDV	People like to work in groups. People like to chat with friends while working. Friendship is highly valued. Relationship-centred society.	2	Unintentional sharing of confidential information
		3	Concealing faults made by friends
High MAS	People experience a higher degree of gender differentiation of roles. The male dominates significantly making females more assertive and competitive.	4	Using any means to reach goals owing to high competition
Low UAI	More open to unstructured ideas and situations. Society may not follow rules laid down to control unexpected situations.	5	Lower priority to information security policy.
		6	Receiving too little information.
Very High LTO	Favours gifts (previous company's information could be used as a gift).	7	Sharing of information depends on the relationship rather than the principle of need-to-know.
		8	Using previous company's confidential information

[a] Expressions used for links are picked up from Hofstede, G. and Hofstede, G. J. (2004)

Table 12: Characteristics of Chinese Respondents

Age:	
Below 20	0
20-29	74
30-39	88
40-49	19
50-59	5
60 or older	0
Sex:	
Male	102
Female	84
Type of business:	
Real estate	7
Manufacturing	119
Services	26
Sales or trade	22
Other	12

Table 13: Severities of Problems in China According to Percentage of Problem-Causing Answers

(n=186)

CD	Original Problem Number	New Problem Number	Overall Severity %
PDI	①	P1	**93.5**
IDV	②	P4	**83.9**
	③	P5	**83.9**
MAS	④	P8	**96.8**
UAI	⑤	P11	**93.5**
	⑥	P12	**83.9**
LTO	⑦	P13	**77.4**
	⑧	P14	**87.1**

SERIOUS PROBLEMS

By summing up the hypotheses of these three separately conducted studies, examined in this study are the potential problems which may be faced by British companies investing in Russia, India and China. The list of these potential problems, the CDs under which the problems were categorized, the overall severities of the problems in Russia, India and China, and their ranks are presented in Table 14. A problem is not always exclusively linked to a certain CD, but may sometimes be shared by different CDs. For example, P2 "Not giving opinions to managers concerning ISM" and P3 "Less consulting or reporting on ISM incidents" could stem from both high PDI, where the less powerful members in a society tend to believe that they have no right to question the authorities, and low MAS, where people hesitate to discuss their opinions with their managers in fear of ruining their relationships with managers, and are thus categorized under both PDI and MAS. In this table the potential problems are renumbered in its second column titled "Problem Number", which refer to the numbers in the "New Problem Number" column of tables 7, 10 and 14. Problems for which more than 50% of their respondents gave problem-causing answers are considered as serious and are emboldened. The problems which were not set for particular countries are marked with "-", while the problems which are not serious are left unranked.

Table 14: Overall Severities and Rankings of Problems in Economically Rising Countries According to Percentage of Problem-Causing Answers

CD	Problem Number	Problem	%			Rank		
			RU	IN	CN	RU	IN	CN
PDI	P1	Unequal distribution of knowledge on company's ISM	14.7	13.3	**93.5**			2
PDI/ MAS	P2[a]	Not giving opinions to managers concerning ISM	35.3	**66.7**	-		5	-
	P3[a]	Less consulting or reporting on ISM incidents	20.6	33.3	-			-
IDV	P4	Unintentional sharing of confidential information	**94.1**	**90.0**	**83.9**	1	1	5
	P5	Concealing faults made by friends	**52.9**	**76.7**	**83.9**	2	3	5
	P6	Less task-centred and more oriented to chat with co-workers.	35.3	-	-		-	-
MAS	P7	Disgruntled employees.	32.4	-	-		-	-
	P8	Using any means to reach goals owing to high competition	-	**53.3**	**96.8**	-	6	1
UAI	P9	Less interest in ISM	-	**83.3**	-	-	2	-
	P10	Unwilling to follow information security policy without complete understanding.	**52.9**	-	-	2	-	-
	P11	Lower priority to information security policy.	-	-	**93.5**	-	-	2
	P12	Receiving too little information.	-	-	**83.9**	-	-	5
LTO	P13	Sharing of information depends on the relationship rather than the principle of need-to-know.	-	-	**77.4**	-	-	8

P14	Using previous company's confidential information	-	**73.3**	**87.1**	-	4	4

Note: The problems which do not apply for a country are marked with "-"

[a] P2 and P3 are found in both PDI and MAS

These results show that problems 4 and 5 are serious in all the investee countries, while problems 8 and 14 are serious in India and China. The fact that the IDV-based P4 and P5 are serious proves that the high *LoP*s concerning IDV for all countries in Table 4 were effective in practically predicting these problems. Also as predicted by the *LoP*s for LTO in Table 4 British companies in India and China may face the LTO-based P14 with the severity and LTO score in India being less than those in China (73.3<87.1, 61<118, respectively). Contrary to what was predicted, however, the MAS-based P8 is serious only in India and China, whereas Russia, which has the highest *LoP* for MAS, does not seem to be having MAS-based problems. It is logical to assume that this discrepancy may be stemming from the fact that moderate through high scores for MAS in India and China playing a more prominent role than *LoP* for the occurrence of this problem. The fact that both the severity and MAS score for India are less than those in China (53.3<96.8, 56<66, respectively) proves this point further. Thus, it can be assumed that even though *LoP* is accurate in predicting problems for the most part, there are occasions when the Hofstede score alone could predict problems. Problems 1, 2, 9, 10, 11, 12 and 13 are also serious in some countries. The ranks of problems show that P4 "Unintentional sharing of confidential information" is the severest in Russia and India, while P8 "Using any means to reach goals owing to high competition" is the severest in China.

In order to explore in depth the reasons for the occurrence of common problems in Russia, India and China, Table 15 looks at the cultural aspects of UK which might lead to these problems. Problems 4 and 5, which are common to all three of these countries, are emboldened. It can be seen that P4 "Unintentional sharing of confidential information" and P5 "Concealing faults made by friends" occur because of the very high IDV of UK as opposed to the very low through moderate scores for IDV in the investee countries (see Table 2). This implies that aspects such as working in groups and valuing friendship highly of the local employees as opposed to the individualistic attitudes of the British managers impede the proper execution of the company's security policy and the implementation of the principle of Need-to-Know resulting in these problems.

Table 15: British Cultural Dimensions Leading to Potential Problems

British Culture	Link[a]	Problem Number
Low PDI	Greater equality between societal levels reinforces cooperative interaction across power levels creating a stable cultural environment.	P1
		P2
		P3
Very High IDV	People have a more individualistic attitude and relatively loose bonds with others. They are more self-reliant and look out for themselves and their close family members.	**P4**
		P5
		P6
High MAS	People experience a higher degree of gender differentiation of roles. The male dominates significantly making females more assertive and competitive.	P2
		P3
		P7
		P8
Low UAI	More open to unstructured ideas and situations. Society may not follow rules laid down to control unexpected situations.	P9
		P10
		P11
		P12
Low LTO	The society believes in meeting its obligations and tends to reflect an appreciation for cultural traditions.	P13
		P14

[a] Expressions used for links are picked up from Reference [11]

RECOMMENDATIONS

Foreign operation should have a unified single policy because business information is to be shared globally without fear of leakage. Even though policy modifications are not allowed, locality should be taken into account in order to maximize the effect of a company's global policy. The result of this study helps to meet this point. This study has taken local culture into consideration in the expansion of business to economically rising countries. In this sense, the result of this study supplements international frameworks such as ISO/IEC 27001 (2005) and the COSO framework (1994) by showing practical countermeasures taking locality into account.

As the very high IDV score of UK as opposed to the very low through moderate scores of Russia, India and China, which results in high *LoP*s for IDV, could lead to P4 "Unintentional sharing of confidential information" and P5 "Concealing faults made by friends", it is recommended to British managers to understand the friendship-oriented, group-based cultures of local workers and thereby, educate these employees about the principle of Need-to-Know and encourage reporting of faults made by friends as reporting of faults would not result in employees or their friends being reprimanded, but instead help in correcting mistakes.

CONCLUSIONS AND FUTURE WORK

Based on the analysis conducted on the results of this study on problems of ISM faced by British companies investing in economically rising countries, it can be concluded that:
(1) The theory of *LoP* predicts problems to a certain extent.
(2) "Unintentional sharing of confidential information" is the severest problem for British companies in Russia and India.
(3) "Using any means to reach goals owing to high competition" is the severest problem for British companies in China.

Future 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 might be interested in studying about the local culture. In this paper, however, the extreme case where managers are unaware of the local culture is assumed and warnings are shown under the highest estimation of risk. From the practical viewpoint, we need to look into the extent to which 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. Moreover, in order to better understand the situations leading to problems of ISM, it is advised to investigate how national culture influences corporate culture. This study could be expanded to cover the rest of the key investors in economically rising countries as well.

REFERENCES

Asai, T. (2007). *Information Security and Business Activities*. Niigata, Japan: Kameda Book Service.

Asai, T. & Fernando, S. (2011). "Human-related problems in information security in Indian cross-cultural environments". *Journal of Japan Society of Security Management*, *25(2)*, (in print).

Asai, T., Fernando, S. & Castillo, J. (2011). "Human-related problems in information security in Russian cross-cultural environments". *International Journal of Japan Association of Management Systems*, (in print).

Asai, T, Qin, Y. and Caibutengdaoriji (2011). "The influence of cultural differences on information security management in Chinese cross-cultural environments". *Journal of Japan Association for Management Systems*, (under review).

Asai, T. & 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. (2008). "*Human Error at the Center of IT Security Breaches*". Retrieved from http://www.newhorizons.com/elevate/network%20defense%20contributed%20article.pdf. Accessed: September, 2011.

Beckmann, D., Menkhoff, L. & Suto, M. (2007). "Does culture influence asset managers' views and behavior?" *Journal of Economic Behaviour & Organization, 67*, 624-643. doi:10.1016/j.jebo.2007.12.001.

Committee of Sponsoring Organizations. (1994). *Internal Control – Integrated Framework*. Retrieved from http://www.snai.edu/cn/service/library/book/0-Framework-final.pdf. Accessed: October, 2009.

Fernando, S., Das, S. & Asai, T. (2010). "Human-related problems in information security in cross-cultural environments – the case of India –". *24th Annual Conference of Japan Society of Security Management*, 115-118.

Hall, E. T. (1976). *Beyond Culture*. NY: Anchor Books.

Harris, S. (2004). *All in One CISSP Certification: Exam Study Guide* (2nd ed.). Berkeley, CA: Osborne/McGraw Hill.

Hofstede, G. & Hofstede, G. J. (2004). *Cultures and Organizations: Software of the Mind*. NY: McGraw-Hill.

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W. & Gupta, V. (2004). *Culture, Leadership, and Organizations, The GLOBE Study of 62 Societies*. CA: Sage Publications.

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

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business*. West Sussex, England: Wiley.

Pronin, E. (2006). "Perception and misperception of bias in human judgment". *Journal of Trends in Cognitive Sciences*, *11*, 37-43. doi:10-1016/j.tics.2006.11.001

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

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

United Nations Conference on Trade and Development. (2010). *World Investment Prospects Survey 2010-2012*. Retrieved from http://www.unctad.org/en/docs/diaeia20104_en.pdf. Accessed: January, 2011.

Waluyan, L., Blos, M., Noguera, S. & Asai, T. (2010). "Potential problems in people management concerning information security in cross-cultural environment – the case of Brazil". *Information Processing Society of Japan Journal, 51 (2)*, 613-623. doi:10.2197/ipsjjip.18.38

Whitfield, G. B. (1997). "*Business across culture: Equality in the workplace*". Retrieved from http://www.expat.or.id/business/equality.html. Accessed: October, 2009.

Yates, M. (2006). "*Cultural differences*". Retrieved from http://www.leadervalues.com/content/details.asp?contentDetailD-255&Type=More. Accessed: September, 2011.

OUT-OF-BAND WORMHOLE ATTACK DETECTION IN MANETS

Sana ul Haq, Faisal B Hussain
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
msis-6.sanaulhaq@mcs.edu.pk, faisalbashir@mcs.edu.pk

Abstract

Mobile Ad hoc Networks (MANETs) are prone to a variety of attacks due to their unique characteristics such as dynamic topology, open wireless medium, absence of infrastructure, multi hop nature and resource constraints. Any node in mobile ad hoc networks operates not only as end terminal but both as an intermediate router and client. In this way, multi-hop communication occurs in MANETs and thus it is a difficult task to establish a secure path between source and destination. The purpose of this work is overcome a special attack called wormhole attack launched by at least two colluding nodes within the network. In this paper we enhance AODV to detect and remove wormhole attack in real-world mobile ad hoc networks. In an out-of-band wormhole attack the communication between two malicious nodes is hidden from the rest of the nodes. This property is exploited by our proposed AODV-DRW protocol for the detection of wormhole attack.

Keywords
MANETs;AODV; Wormhole Attack, Secure Routing

INTRODUCTION

MANET (Mobile Ad hoc Network) is a type of wireless networks that have attracted most researchers towards them as MANETs provide better environment for ubiquitous computing that require no infrastructure without wired accessories (Corson, Maker & Cernicione, 1999).

Such networks can be deployed in a situation where exchange of critical information becomes necessary i.e. consider a military background with solders getting timely strategic and tactical information. Most of the existing routing protocols in MANETs i.e. AODV (Perkins, Belding Royer & Das, 2003), DSR (Jhonson & Maltz, 1996), DSDV (Perkins & Bhagwat,1994), are prone to a variety of attacks (Argyroudis & Mahony, 2003) that can degrade the performance of the whole network and thus pose direct threat to security of such networks, therefore we require solutions that if intruders enter our network, they can be timely detected and prevented before doing any unwanted task. The focus this paper is on the security of routing protocols in MANETs which are the target of the attackers for injecting malicious behavior. In this perspective we work on a special type of routing attack called wormhole (Jhaveri, Parmar, Patel & Shah, 2010) that exploit vulnerabilities in MANETs routing protocols.

Wormhole attack is a network layer attack. In a typical wormhole attack at least two colluding nodes in the network are located at different places that are not in direct communication range of each other i.e. one near to the source node and another near to the destination node thus bypassing information from source node to destination node and disrupting proper routing. In Figure 1, M1 and M2 are two colluding nodes. The malicious node M1 takes data near the source node then tunnels it to M2 placed near the destination node. Communication of data occurs via path having this low latency link all the times due to less number of hops.

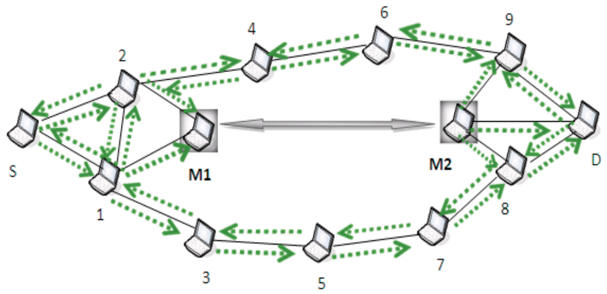

Figure 7 Wormhole Attack in operation

AODV is a reactive routing protocol commonly used in MANETs. In this paper, we have modified Ad hoc on-demand routing protocol AODV to detect and remove wormhole attack. In AODV, when a source node wants to establish a path with destination node, it creates Route Request packet and broadcasts to all its neighboring nodes