Empirical Analysis of Human-Related Problems of Information Security in Cross-Cultural Environments: The Case of the East African Community-

T. Asai[1] and A. U. Hakizabera[2]

[1]Management and Information Systems Engineering, Nagaoka University of Technology, Niigata, Japan
[2]Information Science and Control, Nagaoka University of Technology, Niigata, Japan.
e-mail: asai@kjs.nagaokaut.ac.jp

Abstract

The growing interest in investment towards Africa in the last few years has been remarkable, thanks mainly to the growth of stronger economies and democracies on the continent and to an increased need for raw materials. The East African Community (EAC) composed of Burundi, Kenya, Rwanda, Tanzania and Uganda, presents a good investment platform for foreign investors due to their economies of scale. This paper discusses the potential problems concerning information security, which foreign companies may face in the EAC. UK, US, Belgium, China and Japan are selected as investor countries in this study. The potential problems of each country are examined using Greet Hofstede's framework of cultural dimensions. By using a measure called Level of Potential (LoP) whose practicability has been proved through previous research, the magnitude of the potential problems concerning Information Security Management (ISM) is predicted. We conducted a survey in one of the countries in the EAC, Rwanda, to evaluate the severity of the problems. We found the problem of "using previous company's confidential information" to have the highest severity. A list of countermeasures is proposed to protect business information.

Keywords

Cultural Difference, Cultural Dimension, Information Security, Human-related Problem

1. Introduction

The Internal Control-Integrated Framework of COSO (Committee of Sponsoring Organizations of the Treadway Commission) (1994) refers to ethnical values as a control environment factor in chapter 2, Control Environment. The section of Foreign Operations says, "The expansion or acquisition of foreign operations carries new and often unique risks that management should address." The risks are mostly due to a different cultural environment.

Solms (2005) states that Information Security Management (ISM) should be defined as both technical and non-technical activities. Moreover, Bean (2006) states that eighty percent of information security breaches are caused by human error. In general, people act on their perception which may be influenced by their culture.

According to Hofstede (2004), culture influences people's beliefs and expectations. Schneier (2008) and Komatsu (2008) also state that people's expectations may be one of the causes of misjudgment concerning how to react to risks. Thus, it is natural to think that culture may have some relation to human errors, especially in a cross-cultural environment. There are extensive studies, (Carrel et al. 1995; Hofstede, 2004), concerning cultural impact on the way of business in fields like organizational behavior (OB) and human resources management (HRM). One of the objectives of these fields is to understand better the reasons behind employees' reactions. Thus, unfavorable reactions can be predicted (Carrel et al. 1995). However, no one had carried out a quantitative study on this relationship with the respect to ISM until Asai et al. (2008), who studied the cultural impact on ISM and measured its magnitude by applying a measure they developed, called Level of Potential (LoP).

The East African Community (EAC), the regional intergovernmental organization of the Republics of Burundi, Kenya, Rwanda, Tanzania and Uganda, is chosen as an investee country in this paper because of its rising attractiveness for foreign direct investment (Chalker, 2008). UK, US, Belgium, China and Japan are selected as investor countries in this study, the first three for being among the top investing countries in the region and the last two for being recently active in the region.

If there is a cultural gap between an investee country and an investor country and if foreign managers from the investor country are not aware of that gap, they may face some problems concerning ISM. The purpose of this research is to find what kinds of problems, while implementing information security policy, may take place in foreign companies in the EAC because of cultural differences and to suggest supplemental countermeasures in international frameworks such as COSO and ISO/IEC27001 to protect business information in a cross-cultural environment.

2. Cultural dimensions

There are a wide variety of theories concerning cultural differences, such as those proposed by Hall (1976), Trompenaars (2002), Hofstede (2004) and House (2004). This research has adopted the Hofstede's framework because his framework is the most comprehensive about how the sense of values in workplaces is influenced by culture and because he analyzed a large database which covered almost all the major countries. Based on the cultural data collected, he identified five dimensions and graded 74 countries on indices for each dimension. Yates (2006) interpreted and summarized Hofstede's definitions which are briefly illustrated in Table 1. Table 2 lists Hofstede's scores for the 5 investor countries and the East African region.

In order to clarify the magnitude of cultural dimensions, each one is divided into five degrees; very low, low, moderate, high and very high based on Hofstede's scores (Table 2). For each cultural dimension, the difference between the highest score and the lowest score among the scores of all the countries in Hofstede's list is divided by five equally. Table 2 shows that UK and US have the same cultural degrees while Japan and China show quite different degrees. East Africa has the same degree of LTO as UK and US and the same degree of PDI and MAS as Belgium.

Cultural dimension	**Characteristics**	
	High	**Low**
Power Distance Index (PDI)	The members expect that some individuals wield larger amounts of power than others.	Reflects the view that all people should have equal rights.
Individualism (IDV)	Ties between individuals are loose.	Ties between individuals are tight.
Masculinity (MAS)	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.
Uncertainty Avoidance Index (UAI)	Many rules and low tolerance of deviant ideas, resistance to change.	Few rules and high tolerance of deviant ideas.
Long Term Orientation (LTO)	Persistence, ordering relationships by status, thrift and having a sense of shame.	Personal steadiness and stability, respect for tradition and reciprocation of greetings, favors and gifts.

Table 1: Hofstede's cultural dimensions

CD	**Level**	**Countries**					
		EA	**UK**	**US**	**BE**	**CH**	**JP**
PDI	Very Low						
	Low		35	40			
	Moderate	64			65		54
	High					80	
	Very High						
IDV	Very Low					20	
	Low	27					
	Moderate						46
	High						
	Very High		89	91	75		
MAS	Very Low						
	Low						
	Moderate	41			54		
	High		66	62		66	
	Very High						95
UAI	Very Low						
	Low		35	46		30	
	Moderate	52					
	High				76		
	Very High						92
LTO	Very Low						
	Low	25	25	29			
	Moderate						
	High						80
	Very High					118	

＊EA (East Africa), UK (United Kingdom),US(United States of America), BE (Belgium), JP (Japan), CH (China)

Table 2: Hofstede's scores

3. Research method

3.1. Assumption

It is assumed that foreign managers from an investor country may face some problems in implementing their information security policy if there is a cultural gap between the investee country and the investor country and if the foreign managers are not aware of the gap. In other words, we assume that if foreign managers know the problems (due to cultural differences) that may take place in their cross-cultural workplaces in their visiting investee country, they may find a better way to protect their business information.

3.2. Level of potential

In cross-cultural environments, most problems occur because of the differences between the magnitudes of cultural dimensions. The wider the gap between foreign investor's culture and the local culture is, the higher the likelihood that problems will occur. In order to predict the magnitude of potential for problems, this research uses the LoP which is the extent to which problems may arise because of cultural differences.

$$LoP = |\ CD\ of\ an\ investor\ country - CD\ of\ an\ investee\ country\ |, \ldots\ldots\ldots \quad (1)$$

where LoP = Level of Potential, CD = Hofstede's score of cultural dimension.

In other words, the LoP is the absolute value of the difference between the score of a cultural dimension of an investee country and the score of an investor country, as shown in Formula (1). To have a detailed categorization, considering the difference between the highest score and the lowest score for each cultural dimension in the list of Hofstede's scores, LoP is equally divided into five levels: very low potential (▲), low potential (△), potential (◎), high potential (○) and very high potential (●).

3.3. Approach

1. Set potential problems based on Hofstede's scores for the investee country (EAC in this study) and the authors' experience in foreign companies.

2. Predict potential problems logically by using LoP. LoP is defined as shown by Formula (1). The probability of occurrence of a problem is proportional to its potential.

3. Develop questions related to each potential problem by taking into account the results of Hofstede's study (Hofstede, 2004). Favorable answers to these questions constitute triggers to the potential problems if the answers agree to let them happen. These kinds of answers are defined as favorable.

4. Poll local employees working for foreign companies.

5. Evaluate the severity of the problems based on the collected data.

6. Compare the actual severity with the predicted potential. As far as human-related problems are concerned, the more employees return favorable answers, the higher the probability is and the higher the severity is. Therefore, we can test the validity of LoP with this comparison. This step is, however, not demonstrated in this paper because the validity has already been proved in previous research. Waluyan et al. (2010) proved it by showing a high correlation between logically predicted potential (probability) and empirically surveyed severity.

7. Find which problems may take place, what triggers them and how severe they are.

8. Find countermeasures to cope with the identified triggers.

9. Find solutions to prevent the problems.

4. Potential problems and logical prediction of their potential

Taking into consideration Hofstede's scores for the EAC and the authors' experience of working in foreign companies (one of the authors worked in East Africa and the other used to work for a global company), as well as the analysis in section 2, a set of potential problems was developed. Table 3 lists the relationship between East African cultural dimensions and related potential problems in the EAC.

CD	Links between cultural dimension and potential problems *	Potential problems in EAC	
		No.	**Description**
Moderate PDI	Less powerful members tend to accept that information is distributed unequally.	1	Lack of education about the company's ISM.
Low IDV	People like to chat with friends about their work.	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 opinion to managers concerning ISM.
Moderate MAS	People tend to value good working relationship with their managers. They are afraid of confrontation with their managers	4	Same as above
		5	
	High MAS society is characterized to be assertive and competitive.	6	Using any means to reach goals owing to high competitiveness.
Moderate UAI	In low UAI society, people try to have as few rules as possible and the rules are more flexible.	7	Lower priority to ISM.
	People in low UAI society don't want to know peripheral information	8	Low interest in ISM.
		9	Less interest in information outside duties.
	People are less tolerant of deviant ideas and resistant to changes.	10	Unwilling to understand or follow the policies.
Low LTO	People in low LTO society like favors or gifts. They may use previous company's information as a gift.	11	Using previous company's confidential information.

Note*Adapted from Hofstede, G. and Hofstede, G.J. (2004): JETRO (1999)

Table 3: East African cultural dimensions and potential problems

The LoP of the five investor countries, as illustrated in Table 4, are calculated by using Formula (1). Table 5 shows overall potential [scores] and their base data. The score of overall potential is calculated by aggregating numbers of levels. Numbers 1 through 5 are given to the lowest level (▲) through the highest level (●), respectively. Table 5 is created by marking a country with the mark of the highest LoP if a problem has more than one cause, for example problems 4 and 5. It also reveals that UK, US and Belgium are more likely to face problems due to IDV and MAS. Japan and China are more likely to face problems due to UAI and LTO.

	Level of Potential (LoP)				
	UK	US	BE	CH	JP
PDI	29	24	1	16	10
IDV	62	64	48	7	19
MAS	25	21	13	25	54
UAI	17	6	24	22	40
LTO	0	4	*-	93	55

*Note: No data available

Table 4: Level of Potential

	Problems	UK	US	BE	CH	JP
PDI	1	△	△	▲	▲	▲
IDV	2	○	○	□	▲	△
	3	○	○	□	▲	△
MAS	4	○	○	□	△	□
	5	○	○	□	△	□
	6	△	△	▲	△	□
UAI	7	▲	▲	△	△	△
	8	▲	▲	△	△	△
	9	▲	▲	△	△	△
	10	▲	▲	△	△	△
LTO	11	▲	▲	*-	●	□
	Overall Potential	25	25	22	22	25

*Note: No data available

● very high; ○ high; □ potential; △ low;
▲ very low

Table 5: Predicted potential

5. Empirical analysis of potential problems

5.1. Profile of survey

Rwanda, one of the countries in the EAC, was chosen as a pilot country for the survey in order to evaluate the severity of potential problems that might occur between the EAC and investors. We selected Rwanda because it shares the same cultural dimension with the other countries in the EAC and for that reason, Hofstede's list treats the East African countries as a single entity. Moreover, the Rwandan respondents were immediately accessible at the time of the study. Because of the similarity of the cultural dimension in the EAC, we assume that the results from Rwanda are applicable to the other countries in the same community. We carried out a survey in December 2009 by interviewing 30 Rwandan employees working for foreign companies on their attitudes towards ISM. The objective of the survey was to find the problems between local employees and their foreign managers. Their profiles are described in Table 6. Most of the respondents are educated, Christian, and in their 20's and 30's. We do not intend to derive any conclusions concerning these characteristics as they are not relevant to the objectives of this study.

Sex		**Age**		**Religion**		**Business type**	
Male	63.3	20-29	70.0	Christian	96.7	Financial	33.4
Female	36.7	30-39	26.7	Others	3.3	Technical and IT	30.0
		40-59	3.3			Health/Social	13.3
						Education	6.7
						Others	16.6

Table 6: Characteristics of respondents (%)

5.2. Development of questions

Referring to the results of Hofstede's study (Hofstede, 2004), we developed questions to find the magnitude of the severity of the potential problems. These questions constitute conditions to make the potential problems happen in real environments. As illustrated in Table 7, the developed questions are related to the potential problems. Each question has its favorable (not always affirmative) answer which triggers the related problem. A problem is considered as serious if more than 50% of respondents give favorable answers. According to the survey, six problems (marked gray in the table) are more serious than the others and represent more of than half of the predicted problems.

5.3. Analysis of serious problems

The survey shows the magnitude of the severity of the problems that may emerge in the EAC. Problem 4 and Problem 5 are both related to IDV and MAS cultural dimensions as shown in Table 3. This section focuses on the problems judged more serious among the developed problems. They are Problems 1, 2, 6, 7, 8 and 11 (Table 7).

Problem 1: Lack of education about the company's information security management (PDI-originated problem).

There are two questions, the answers to which are accepted as conditions for Problem 1 (Table 7, Q1 and Q2). The favorable answers to the two questions show that there is a tendency that subordinates do not care about the company's information security management because they think that ISM should be addressed to managers rather than to themselves. However, information security should be everyone's business. They would also prefer to have fewer meetings to be held in their company. The lack of interest translates into a lack of knowledge about ISM. The LoP of Problem 1 shown in Table 5 indicates that British and American companies have higher potential to face this problem compared to Belgian, Chinese or Japanese companies. British and American companies would expect all the employees to be equally educated on what they consider important.

Problem 2: Unintentional sharing of confidential information (IDV).

There are four questions (Table 7, Q3, Q5-Q7), the answers to which are accepted as conditions for Problem 2. These four conditions, which have comparatively high percentages of favorable answers, show tendencies towards information sharing as employees regard it as natural. This problem seems to be due to their high collectivism society. The LoP of Problem 2 shown in Table 5 suggests that low collectivism investor countries like UK, US and Belgium may have higher potential to face that problem than China and Japan which share almost the same collectivism behavior as the EAC.

Problem 6: Using any means to reach goals (MAS).

There are three triggering conditions for Problem 6 (Table 7, Q13-Q15). These triggering conditions show a tendency for employees to work as much as possible to reach their goals.

(December, 2009; n= 30)

CD	Pbl	Questions	FA%
PDI	P1	Q1. Meetings are too often held.	83.3
		Q2. Workers should not be burdened with information security-related activities; there should be a specific department to deal with it.	73.3
		P1 Average	78.3
IDV	P2	Q3. I don't mind sharing any skill or knowledge with my coworkers.	76.7
		Q4. I can share my password with a trusted coworker.	23.3
		Q5. Sometimes I like sharing something concerning my job with others.	80.0
		Q6. Information spreads easily in the company.	93.3
		Q7. It is better to share a piece of information than keep it to yourself.	83.3
		P2 Average	71.3
	P3	Q8. I hardly ever decline to help my coworkers even if it is not my job	60.0
		Q9. I place high priority on company's rules above friendship.	23.3
		P3 Average	41.6
	P4	Q10. If I am asked whether I understand a policy or not, I will probably say, "Yes."	10.0
	P5	Q11. I agree to whatever my superior decides without discussion even if I think he's wrong	10.0
		Q12. I don't hesitate at any time to consult my supervisor about my job activities.	10.0
		P5 Average	10.0
MAS	P4	Q10. If I am asked whether I understand a policy or not, I will probably say, "Yes."	10.0
	P5	Q11. I agree to whatever my superior decides without discussion even if I think he's wrong	10.0
		Q12. I don't hesitate at any time to consult with my supervisor about my job activities.	10.0
		P5 Average	10.0
	P6	Q13. I want to continue my work even after working hours have ended.	73.3
		Q14. I often take my work home to please my supervisor by finishing everything in time.	53.3
		Q15. I can bring any document to my home; I am responsible for my actions.	60.0
		P6 Average	62.2
UAI	P7	Q16. Rules should be flexible.	83.3
	P8	Q2. Workers should not be burdened with information security-related activities; there should be a specific department to deal with it.	73.3
	P9	Q17. I am not reluctant to share information even if I'm not asked to.	46.6
	P10	Q18. I can adjust myself easily to any new policy without a doubt.	13.3
		Q19. If a new policy is contrary to my personal belief, I will not follow it.	30.0
		P10 Average	21.6
LTO	P11	Q20. The skills and knowledge that I have acquired personally at work are my valuable assets. Therefore I am free to use them even after moving to another company.	100.0
		Q21. According to my morals and values, teaching others with my personal experience and knowledge is a good thing to do.	100.0
		P11 Average	100.0

Table 7: Survey results and severity of problems

Note: CD: Cultural dimension Pbl: Problems FA: Favorable answers

When employees are persistent in working late and taking documents home, they can unconsciously leak information about their company or perform some illegal actions for the sake of competitiveness and good performance. Japan, which is known to be a very masculine society (Table 2) that encourages a very competitive behavior, has the highest potential of facing this problem.

Problem 7: Lower priority to information security management (UAI).

Question 16 “Rules should be flexible” is the question to which an affirmative response is accepted as a condition for Problem 7 (Table 7). The answers show that employees have a tendency to prefer rules that are more flexible. That suggests that they may not give particular priority to information security. The LoP of Problem 7 shown in Table 5 and the scores shown in Table 2 indicate that Belgian and Japanese companies which have a lower tolerance for uncertainty, have slightly higher potential to face this problem than British or American companies.

Problem 8: Low interest in information security management (UAI).

The results demonstrate that workers show low interest in information security management and think that it should be assessed by a specific department (Table 7, Q2). Belgian and Japanese companies have more potential to face this problem.

Problem 11: Using previous company's confidential information (LTO).

The two triggering conditions (Table 7, Q20 and Q21) reveal that information, knowledge and skills acquired in companies are unanimously considered by workers to be their own. In addition, sharing their experience and knowledge is encouraged by their morals and values. This encourages the use of a previous company’s confidential information which is a big threat to foreign investor countries. China is found most likely to face LTO-originated problems, followed by Japan (Table 2, Table 5).

6. Conclusions and future work

From the findings mentioned above, it can be deduced for the EAC that:

- The problems that may arise in British companies may also arise in American
- companies because of their cultural similarity.
- British, Belgian and American companies have higher individualism-originated
- potential problems than Japanese or Chinese companies.
- Japanese companies have the highest potential in facing problems due to MAS.

- The highly competitive environment that Japanese companies may create can push the workers to be careless about the manipulation and storage of information.
- Belgian and Japanese companies which are stricter about the rules are likely to face more UAI-originated problems than American or British companies. Chinese companies have the highest potential to face problems due to LTO.
- Overall, British, American and Japanese companies are found to have higher potential to face problems in EAC. However Belgian and Chinese companies are not far behind.
- With 100% of favorable answers, the problem of "using a previous company's confidential information" has been found to have the highest severity.

Problems and recommendations
"Lack of education about the company's information security management": - Emphasize the importance of attending meetings to learn more about ISM. - Make employees participate in discussions to increase their awareness.
"Unintentional sharing of confidential information": - Explain to employees that information sharing is a breach of security if it is against Need-to-Know principle.
"Using any means to reach goals": - Explain to employees that they need to obey rules even if they think the purposes of their actions are right or may increase their performance.
"Lower priority to information security management": - Give employees the proper understanding that a threat of information leakage may occur anytime and anywhere. They have to follow rules without any exception.
"Low interest in information security management": - Make employees understand that ISM is not only a matter of technology but also a matter of human resource management and that is everybody's business.
"Using previous company's confidential information": - Convince employees that "teaching others" is not always good in practice of ISM. - Give employees the proper understanding that any knowhow acquired in their companies is not their assets but their companies'.

Table 8: Problems and recommendations

We recommend that ISO/IEC 27001 should state the necessity of managing change in foreign operations more clearly. It refers to the security concerning human resources mainly in regards to employment, but it does not mention anything about the influence of cultural differences. Even though the COSO (1994) framework refers to the influence of cultural differences, it doesn't offer any practical recommendations. Based on the problems mentioned previously, several actions can be recommended to the potential investor in the EAC as shown in Table 8.

We are planning to carry out more detailed analysis on a larger sample size and find the correlations between potential problems and local workers' characteristics.

7. References

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, 15-26.

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).

Carrel, M.R., Elbert, N.F. and Hatfield, R.D. (1995), Human Resource Management: Global Strategies for Managing a Diverse Work Force, Prentice Hall, New Jersey, ISBN-13: 978-0023195334.

Chalker, B.L. (2008), "East Africa - A rising investment destination", http://www.

africamatters.com/ news.asp?page_id=204&n_id=85 (Accessed 06 December 2009).

Committee of Sponsoring Organizations of Treadway Commission (1994), "Internal Control – Integrated Framework", http://www.snai.edu/cn/service/library/book/0-Framework-final.pdf (Accessed 17 February 2010).

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.

JETRO (1999), "Communication with Japanese in business", http://www.jetro.co.jp/france/lyon/pdf/cwjb.pdf (accessed 15 December 2007).

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

Solms,V. (2005), "Information security governance – compliance management vs. operational management", Journal of Computer and Security, 24 , 443-447.

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,Vol.51,No.2, 613-623.

Yates,M.(2006), "Cultural differences", http://www.leadervalues.com/content/detail.asp?contentDetaillD-255&Type= More (Accessed 02 December 2008).