Exploring the Influence of National Cultures on Non-Compliance Behavior

Taco Dols
International Flavors & Fragrances, Inc.
taco.dols@iff.com

A.J.Gilbert Silvius
Utrecht University of Applied Sciences
gilbert.silvius@hu.nl

ABSTRACT

IT organizations and CEO's are, and should be, worried these days about the (lack of) data confidentiality and the usage of 'shadow' IT systems by employees. In addition to the company's risk of monetary loss or public embarrassment, the senior management themselves increasingly risk personal fines or even imprisonment. Several trends reinforce the attention for these subjects, including the fact that an increasing number of employees perform parts of their work tasks from home (RSA, 2007) and the increasing bandwidth available to users which makes them rely on the Internet for satisfying their business and personal computing needs (Desisto et al., 2008). Employees' complying with the existing IT security policies is therefore essential.
This paper presents a study on one of the factors that influence non-compliance behavior of insiders or employees in organizations: National Culture. The expected influence derived from researching literature have been tested in a survey study amongst employees of a big-5 accountancy firm in the Netherlands and Belgium. The study concludes that cultural aspects are indeed important factors influencing non-compliance behavior, but that not all expectations were confirmed.

Keywords
Information Systems Security, Non-Compliance, Culture.

INTRODUCTION

Information security is a widely discussed topic these days (e.g., Brooke, 2004; Gordon, 2005; Ponemon Institute, 2007). Despite years of investments in technology and processes, truly protecting data remains a distant goal for information security officers (Al Awadi & Renauld, 2007). Figuring out what, when and how to protect has become very complex and has created the need for a new approach, which includes establishing meticulous risk fundamentals and which requires using a holistic technical understanding (Richards, 2008). New technological developments such as Software-as-a-service, Web 2.0 technologies and multi-media hardware like iPhones increase the number of possibilities for sensitive information falling in the wrong hands. To make matters worse, some companies are decreasing budgets in IT security

in order to reduce cost, and recent lay-offs have increased the risk of disgruntled employees taking off with sensitive data (Gage, 2009).
The risk is real and the problem is huge: In a 2009 survey among IT managers in the U.S. and Europe, almost all respondents, 98%, said their organization has experienced tangible loss as a result of a cyber attack incident and 31% experienced theft of customer or employee personally identifiable information. Another 25% were hit with theft of corporate data (Symantec, 2009). And according to another study (Verizon, 2009) more electronic records were breached in 2008 than the previous four years combined, most by organized crime. Besides threats from malicious outsiders (hackers), there are also malicious and negligent insiders (employees). A large worldwide survey (Ernst & Young, 2009) shows that the economic crisis has increased the number of ex-employees stealing or intentionally destroying data (malicious insiders).
Despite the threats from malicious in- and outsiders, negligence and carelessness amongst employees still pose the greatest security threat to a company (e.g., Ponemon Institute, 2006; Whitty, 2006; Krom, 2006; Moreau, 2007; Burke and Christiansen, 2009). For example the carelessness with which employees approach data security and the usage of 'shadow' IT systems like USB memory devices, or the use of public collaboration facilities like Google docs. When this careless or negligent behavior is ignoring the organization's IT security policies, we talk about 'non-compliance' behavior. As an important factor influencing this non-compliance behavior, Rundmo et al. (2004) identify the culturally determined attitude towards the company policies and the perception of risk by the employees. As a specification of this, this paper reports a study on the influence of national cultures on non-compliance behavior of insiders or employees.
The structure of the paper is as follows. After a review of the concepts of non-compliance behavior and national cultures, the effect of national culture is tested in a survey study amongst employees of a big-4 accountancy firm in the Netherlands and Belgium. The results of the study are presented and analyzed. The final section of the paper presents the conclusions and limitations drawn from the study.

NON-COMPLIANCE BEHAVIOR

When looking at the concept of IT security, often a distinction is made between technical risk factors and human risk factors (Ponemon Institute, 2007; Sherman, 2004; Schaffner, 2007). Non-compliance behavior can be classified as one of the human risk factors. Non-compliance behavior can be defined as risk taking behavior, deliberate or not-deliberate, by insiders or employees that ignores an organization's (security) policies and guidelines. Several studies have been conducted to find out what causes employees not to follow the IT security policies and guidelines (e.g., Siponen, 2000; Wold, 2004; Cumps et al., 2007).
A review of the existing literature resulted in five influencing factors: Carelessness; Lack of Awareness; Stricter IT Governance; Poor Business – IT Alignment; (National) Culture. Table 1 shows these factors and their source.

Risk factor	*Description*	*Source*
Carelessness	Failure to realize the risk and consequences related to non-compliance behavior.	Ponemon Institute (2007), RSA (2007)
Lack of Awareness	Lack of knowledge and understanding of risks and consequences of non-compliance behavior and company policies related to security and compliancy.	Witty and Wagner (2005), Ponemon Institute (2007), RSA (2007)
Strict IT Governance	Strict control of the work performed by IT professionals, compliance with internal policies or regulations, justification of IT spending, accountability and/or transparency.	Moreau (2007), Lutchen (2004), Cumps et al. (2007)

Poor Business-IT Alignment	Poor alignment to the IT needs and requirements of business professionals is reportedly a factor in the use of non-official IT and inadequate data security.	Spafford (2004), Raden (2005), Moreau (2007), Schaffner (2007) , Cumps et al. (2007), Hung et al. (2007)
(National) Culture	A person's culturally influenced attitude towards risk and compliancy.	Al Awadi and Renaud (2007), Björck and Jiang, Chaula (2006), Mathieson (1991), Rundmo et al. (2004)

Table 1. Overview of factors influencing non-compliance behavior.

Although several studies identify (national) culture as one of the influencing factors, more in-depth research on cultural related aspects influencing information security is scarce. The human factors, such as culture, have rarely been investigated (Al-Awadi and Renaud, 2006), but the importance of information security in an organization makes it clear that technology alone cannot lead to sufficient solutions and that human aspects cannot be isolated from technology (Slay, 2003).

NATIONAL CULTURE

Hofstede (1991) defines culture as "the collective programming of the mind, which characterizes the members of one organization from others." By "collective programming" Hofstede refers to the symbols, heroes, rituals and values that collectively define a culture. Symbols are specific words, gestures, objects of status symbols that carry a particular meaning to people of the same culture. Heroes are people, real or imaginary, dead or alive, that have the ability to influence behavior based on their status, skills or charisma. Rituals are activities that in itself are seemingly unnecessary, but in the culture are considered essential. Symbols, heroes and rituals are the practices of a culture. They are visible and observable to an outside spectator. At the core of a culture lie the values. Values are "broad tendencies to prefer certain states of affairs over others" (Hofstede, 1991). They represent how things "ought to be".
Cultures come in many different kinds or layers, such as national cultures, organizational cultures, organizational subcultures and occupational cultures (Gefen and Straub, 1997; Hofstede, 1991). Organizational culture represents values that are dominant in a particular organization. Robbins (2005) argues that national culture, organizational culture and employee behavior can be correlated and that national culture influences employee more than organizational culture. Therefore, knowledge about national culture is vital if accurate prediction of employee behavior in an organization is sought. In this view, if an organization plans to develop an effective security culture, it should not be developed in isolation of national culture and the organizational culture (Chaula, 2006).
In this paper we investigate the impact of national cultures on non-compliance behavior. We rely on Hofstede's work to understand more about the concept of national culture. Based on a survey of more than 50 countries involving more than 120,000 respondents. Hofstede (1980) presented a framework of dimensions of national cultures, This framework characterizes culture on the following four dimensions:

PDI (Power Distance Index)

> The basic issue involved within this dimension is human inequality. A national culture characterized by high power distance is more willing to accept inequalities (e.g. those between a manager and her/his subordinates) within an organization than cultures with low power distance.

IDV (Individualism vs. collectivism)

> In cultures that are considered highly individualistic, individuals are loosely tied and are expected to look out for themselves and their family. In 'collectivist' cultures, people are integrated into strongly cohesive in-groups, and group loyalty lasts a lifetime. In individualistic cultures, time,

punctuality and schedules are considered highly important, whereas in collectivistic cultures personal relationships and contacts prevail. In countries such as the USA, individualism is seen as a blessing and a source of well-being while in others, such as China, it is perceived as alienating.

MAS (Masculinity vs. femininity)

In the dichotomy masculine versus feminine, a masculine culture values assertiveness, performance and material success. In a feminine society values like quality of life, tenderness and modesty prevail. In a feminine culture, individuals don't like to stand out or be unique, whereas in a masculine society success and career are valued highly.

UAI (Uncertainty Avoidance Index)

The uncertainty avoidance index is defined as "the extent to which the members of a culture feel threatened by uncertain or unknown situations" (Hofstede, 1991). Low UAI cultures try to minimize the possibility of uncertain, unexpected situations by strict laws and rules, safety and security measures.. Cultures with a low UAI are less rule-dependent and are more trusting (Mooij, 2000).

Based on follow-up research among students in 23 countries around the world, and criticism that the model represented a very 'western' way of thinking (Bond, 1984), a fifth dimension was added.

LTO (Long Term Orientation vs. Short Term Orientation)

Long Term Orientation is characterized by persistence, ordering relationships by status and observing this order, thrift, and having a sense of shame, whereas short-term orientation is characterized by personal steadiness and stability, protecting your 'face', respect for tradition and reciprocation of greetings, favors, and gifts.

Hofstede's framework may not be perfect, e.g. the omission of former Eastern European countries in the study has been criticized (Miller et al., 2006), and some authors (Miller et al., 2006; Smith & Bond, 1998) prefer alternative frameworks such like Schwartz's (1994). We, however, use Hofstede's framework in this study because it is widely known and used among both academics and practitioners., and the positions of the respondents in our study, management level professionals within an IT context, closely resemble Hofstede's respondents. In addition, alternative frameworks, like Schwartz's, achieved a refinement of Hofstede's work, rather than a contradiction (Miller et al., 2006).

NATIONAL CULTURE AND IT SECURITY

National Culture influences the way IT is perceived or used. Several authors found proof of this in their studies. Table 2 provides an overview of some studies in this field.

Authors	*Main findings*
Straub (1994)	The author studied the effect of culture on IT diffusion of email and fax in Japan and the United States. His findings suggested why there are differences in email usage and choice among knowledge worker in different cultures.
Livonen, Sonnenwald, Parma, and Poole-Kober (1998)	The authors studied Finnish and American college students that collaborated in a common course using electronic discussion groups. Findings of the study show that cultural attitudes toward technology may influence people's beliefs and use of the

	technology.
Leidner, Carlsson, Elam, and Corrales (1999)	This study examined whether cultural differences influence perceptions of the relationship between Executive Information Systems (EIS) use and decision-making outcomes. The authors compared the responses from in Mexico, Sweden, and the United States. The study found significant differences, predicted by cultural factors, in the impact of EIS use on management decision-making.
Hofstede (2000)	The paper investigates the specific attributes of countries that influence ICT adoption speed. Findings show that cultural variables (individualism and uncertainty avoidance) can be used to predict the ease and speed of changes. Cultures of high uncertainty avoidance are slow of adopting new technologies.
Veiga, Floyd and Dechant (2001)	This study discussed the effects of national culture on the acceptance of IT, using the Technology Acceptance Model (TAM). The authors compared acceptance in Japan and the United States and the findings suggest that Hofstede's dimensions of cultural differences play distinct roles in influencing the acceptance.
Png, Tan and Wee (2001)	This study compared the adoption of frame relay between the United States and Japan. The findings suggest that uncertainty avoidance, one of Hofstede's dimensions, affected the adoption decision of companies differently in the two countries.
Birgelen, Ruyter, Jong and Wtzels (2002)	The authors compared ICT use in after-sales service-and-support operations in Sweden, Belgium, France, Spain, Austria, Ireland, Netherlands, United Kingdom, Norway, and the U.S. The findings suggest that cultural characteristics will partly determine the design of effective after-sales service contact modes.
Sørnes, Stephens, Sætre, and Browning (2004)	The authors studied how workers in Norway and the United States use information and communication technology (ICT). Their findings show that ICT use reflects Hofstede's findings for PDI and UAI, but that it doesn't reflect cultural differences for IDV and MAS.
Waarts and van Everdingen (2005)	This study investigates if national culture adds to the explanation of differences in adoption of innovations for firms operating in different countries. The authors performed a large-scale empirical study in 10 European countries concerning the adoption of Enterprise Resource Planning (ERP) software by medium-sized companies. Key finding is that variables describing national cultural highly significantly explain variance in adoption decisions in addition to the traditional micro and meso variables.
Miller, Batenburg and van de Wijngaert (2006)	This study investigates the adoption rates of ERP systems from fourteen European countries. The study explores if a national cultural framework could be used to explain the differences. The framework used was Schwartz's seven national cultural value types. After controlling for industry and size, it was found that conservatism has a negative relationship while autonomy, egalitarian commitment, and harmony have a positive relationship with the adoption of ERP systems.
Batenburg (2007)	The author explored country differences in adoption of electronic procurement. Analyses are conducted on 3475 organizations from seven different European countries. The study concludes that there indeed are country differences with respect to e-procurement adoption, and that firms from countries with a low uncertainty avoidance such as Germany and the UK are the early adopters of e-procurement, while countries that are less reluctant to change such as Spain and France have lower adoption rates.

Van Decrean (2007)	The author studied cultural differences in websites in Germany and the United States, using Hofstede's framework. His findings suggest a reflection of national cultures in the websites of international companies.

Table 2. Summary of Comparative Studies of cultural impacts on IT practices.

All of the studies listed in table 2 show a certain impact of national cultures in the perception and use of IT. Given these findings it should therefore be expected that national culture also influences the security of IT and business. This influence however is not reflected in many studies on IT security so far. Björck and Jiang (2006) in their study "Information Security and National Culture" make a first attempt in this direction and Al-Awadi and Renaud (2007) establish a link between trust (in IT) and culture. According to Gartner (Witty et al., 2001) trust is "the result of applying a combination of authentication, authorization, integrity and non-repudiation controls, in other words: trust results from the effective application of information security techniques."

THE STUDY

In the study reported in this paper, culture was tested as a factor influencing non-compliance behavior by means of a survey conducted amongst employees of one of the 'Big Four' accounting firms in The Netherlands and in Belgium between December 2008 and February 2009. The selection of Belgium and the Netherlands was inspired by the substantial differences on three of the four Hofstede's culture variables by these neighboring countries.
Within Europe, several cultural streams are found, each with its distinct cultural dimensions. For instance, The Netherlands in general is said to be in the Germanic region (West Slavic, West Urgic), together with Germany, Austria and Switzerland. It is characterized as having a medium IDV, a low PDI, a medium to high UAI and a medium to high MAS (Nath and Sadhu, 1988). Belgium, through its 'language barrier' is split in a Flemish and Walloon part which represents respectively the Germanic and Latin culture. As the respondents were mostly located in the Walloon part, for this paper the Latin culture is applied to Belgium, which is shared with the French, Spanish, Portuguese and Italian. It is characterized as having a medium to high IDV, a high PDI, a high UAI and a medium MAS (Nath and Sadhu, 1988). Table 3 shows the culture dimensions of the Netherlands and Belgium (Hofstede, 2008).

	PDI Power Distance Index	IND Individualism vs. Collectivism	MAS Masculinity vs. Femininity	UAI Uncertainty Avoidance Index
Maximum score (all nations)	104	91	110	112
Minimum score (all nations)	11	6	5	8
Score for the Netherlands	38	80	14	53
Score for Belgium	65	75	54	94

Table 3. Belgium and the Netherlands compared on Hofstede's variables
(Note: Because of the fact that Belgium does not have a score on Hofstede's long term orientation vs. short term orientation variable, this dimension was discarded in the study.)

Based on the cultural characteristics of the two countries in the study, we can now specify the expected relationships between non-compliance behavior and national culture for the Netherlands and Belgium.

Expected results

Based on the Hofstede (1980) descriptions, some theories can be formed about the attitude and behavior of the employees in the respective countries in relation to their culture.

PDI Power Distance Index

Many organizations employ the Power Distance Index (PDI) to measure the hierarchical relationships between subordinates and leaders such as respect for authority. The PDI can be viewed as an organizational leadership style, being either autocratic or participative (Hofstede 1980). One notices that Belgium has an above-(European) average PDI score compared to The Netherlands, who has a below-average score.

In a high PDI-culture, the leader is expected to provide detailed instructions on tasks since the subordinates expect the leader to lead. Like in the military, a leader in a high PDI culture would also expect orders to be followed without questions asked (Odubiyi, 2006). Low PDI cultures are characterized by leadership styles that empower subordinates and treat them with respect. These characteristics are usually evident in "Good to Great" companies, such as Kimberly-Clark, General Electric, Walgreens, and Gillette (Collins 2001). It should therefore be expected to find different results for the Netherlands and Belgium on the questions in the survey that relate to the compliance to the organization's policies or a manager's instructions. On these questions one would expect higher average scores for Belgium compared to The Netherlands.

IDV Individuality Index

The index score on this variable do not differ a lot. Actually, both countries score above the European average. A high IDV index value indicates that the population has a more independent nature and tends not to 'meddle' in the matters of others. Therefore on questions that concern the correction of non-compliance behavior of colleagues, one would expect most respondents of both countries to respond negatively.

As with Power Distance Index, which is relatively low, and IDV, which is relatively high, it would be expected that not many employees would execute orders if they know that these are in conflict with the existing security policies.

MAS Masculinity Index

The Netherlands have a very low MAS compared to Belgium and compared to the European average. It is hard to predict what effect this would have on the outcome of the surveys. Surveys show that women show different behavior when using IT devices and usage of Internet (for example Fallows 2005; Whitty 2006; Harris 2006) and in high MAS countries women are more prone 'to behave like man'.

Mooij (2002) found that feminine cultures extend their need for quality of life into the workplace as well. Leisure and personal activities, such as reading the news and watching television, may be tolerable at work. This is not so in masculine cultures, where one would find a stricter task orientation. Employees in feminine cultures are also likely to take work home just to be with their families.

UAI Uncertainty Avoidance Index

Belgium has a high UAI value compared to the Netherlands and to the European average. In such societies, strict policies, and regulations are adopted and implemented, in order to eliminate or avoid the unexpected. On questions that test a person's own judgment against the organization's

policy, a high UAI culture would therefore be expected to prefer the 'safe' route of the organization's policy. Based on research by Hofstede (1980), it can be expected that the Dutch respondents, with their low Power Distance score, would show limited acceptance of power inequality and higher assertiveness than Belgians. That would include behavior such as ignoring IT security rules "if they don't make sense", refusing to execute tasks if they feel these are against personal beliefs and less resistance towards addressing observed security breaches with peers.

Again referencing to Hofstede, it is observed that the Dutch have a very low Uncertainty Avoidance score compared to Belgium and the European average. Low UAI cultures are less rule-dependent and more trusting. This may lead to experimentation with new online applications or software. Also, companies in low UAI countries are less likely to impose strict company rules on ICT usage, and if they do, it's likely that people will challenge or break such rules for pragmatic reasons (Veiga et al., 2001).

Research design

The empirical part of our study was aimed at testing the expected influences of national culture on non-compliance behavior. For this purpose, a survey study was designed that consisted of 15 questions. In the survey, 5 general descriptive questions were asked and 10 questions were designed to test whether the respondent actually showed non-compliance behavior. Table 4 shows the design of the questionnaire.

Question		Type of question	Values
Descriptive questions			
1	Gender	Single select	[Male] [Female]
2	Country of origin	Single select	[Belgium] [the Netherlands]
3	Age Group	Single select	[18-23] [24-29] [30-35] [36-41] [41+]
4	Company laptop	Single select	[Yes] [No]
5	Number of years with the company	Single select	[<1 yr] [1-3 yr] [4-6 yr] [>6 yr]
Questions to test non-compliance behavior.			
6	Please rate your familiarity with the security policies for your organization.	7-step semantic differential	Very Familiar to Very Unfamiliar
7	Do you practice the IT security policies of your organization?	7-step semantic differential	Always to Never

8	I sometimes need to bend the rules in order to get work done.	7-step semantic differential	Strongly Agree to Strongly Disagree
9	I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	7-step semantic differential	Strongly Agree to Strongly Disagree
10	If the IT security rules make no sense to me, I sometimes ignore them.	7-step semantic differential	Strongly Agree to Strongly Disagree
11	I use Google Docs or other on-line collaboration software to store or share work with colleagues.	7-step semantic differential	Often to Never
12	I sometimes send documents (that could be considered to contain sensitive/confident ial information) to a home/private email account so I can work from home.	7-step semantic differential	Strongly Agree to Strongly Disagree
13	If my manager asks me to bend the IT security rules, I will do so.	7-step semantic differential	Strongly Agree to Strongly Disagree
14	If I notice a colleague not following the IT security guidelines, I will address this with him/her.	7-step semantic differential	Strongly Agree to Strongly Disagree
15	I store or transport documents (that could be considered to contain sensitive/confidential information) on portable storage like a USB stick (excluding company issued encrypted devices).	7-step semantic differential	Often to Never

Table 4. Design of the questionnaire.

Respondents

The invitation to participate in this survey was sent out to 653 randomly selected employees: 361 in The Netherlands and 292 in Belgium. The respondents were asked to fill out a questionnaire by means of a Computerized Self- Administered Questionnaire (Babbie, 2003). In total 246 surveys were completed (124 for the Netherlands, 122 for Belgium), corresponding with a response rate of 42.1% (34.3% for the Netherlands, 41.8% for Belgium). Table 5 provides the descriptive statistics of the respondents.

Question		Values	Response [%]
1	Gender	[Male] [Female]	55 45
2	Country of origin	[Belgium] [the Netherlands]	49 51

3	Age group	[18-23] [24-29] [30-35] [36-41] [41+]	8.8 42.9 23.8 9.2 15.4
4	Company laptop	[Yes] [No]	93 7
5	Number of years with the company	[<1 yr] [1-3 yr] [4-6 yr] [>6 yr]	19.8 32.2 15.8 32.2

Table 5. Descriptive statistics of the respondents.

Based on these descriptive data, the respondents are considered representative for the population of the company.

Results

Table 6 shows an overview of the results.

Question	Country	N	Mean	Std. Dev.	Difference of Mean
Please rate your familiarity with the IT security policies for your organization.	Netherlands	124	5,04	1,192	,598
	Belgium	122	4,44	1,336	
Do you practice these policies?	Netherlands	124	5,22	1,213	,169
	Belgium	122	5,05	1,246	
I sometimes need to bend the rules in order to get work done.	Netherlands	124	3,48	1,388	,467
	Belgium	122	3,02	1,379	
I sometimes need to share my passwords with colleagues (excluding identified GTS personel) so they can assist me with my tasks.	Netherlands	122	2,25	1,736	-,060
	Belgium	121	2,31	1,548	
If the IT security rules make no sense to me, I sometimes ignore them.	Netherlands	124	3,66	1,385	,489
	Belgium	122	3,17	1,481	
I have used Google Docs or other on-line collaboration software to store or share work with colleagues.	Netherlands	122	1,63	1,194	,036
	Belgium	121	1,60	1,107	
I sometimes send documents (that could be considered to contain sensitive/confidential information) to a home/private email account so I can work from home	Netherlands	122	2,03	1,605	-,025
	Belgium	121	2,06	1,624	
If my Partner or manager asks me to bend the IT	Netherlands	124	3,35	1,525	-,481

security rules, I will do so.	Belgium	122	3,83	1,723	
If I notice a colleague not following the IT security guidelines, I will address this with him/her.	Netherlands	122	4,25	1,458	,238
	Belgium	121	4,02	1,472	
I have stored or transported documents (that could be considered to contain sensitive/confidential information) on portable storage like a USB stick	Netherlands	122	2,67	1,909	-,402
	Belgium	121	3,07	1,924	

Table 6. Results (Mean and Standard Deviation).

The results show that the Belgium and the Dutch respondents sometimes score substantially different on the questions. The significance of these differences were tested using Levene's test for equality of variances and t-test for equality of means. Table 7 shows the results of these tests.

	Levene's Test for Equality of Variances		t-test for Equality of Means						
								95% Confidence Interval of the Difference	
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Please rate your familiarity with the IT security policies for your organization.	6,819	,010	3,703	244	,000	,598	,161	,280	,916
Do you practice these policies?	,025	,875	1,075	244	,283	,169	,157	-,140	,477
I sometimes need to bend the rules in order to get work done.	,059	,808	2,650	244	,009	,467	,176	,120	,815
I sometimes need to share my passwords with colleagues (excluding identified GTS personel) so they can assist me with my tasks.	1,257	,263	-,284	241	,777	-,060	,211	-,476	,356
If the IT security rules make no sense to me, I sometimes ignore them.	1,917	,167	2,677	244	,008	,489	,183	,129	,849
I have used Google Docs or other on-line collaboration software to store or share work with colleagues.	,100	,752	,244	241	,807	,036	,148	-,255	,327
I sometimes send documents (that could be considered to contain sensitive/confidential information) to a home/private email account so I	,052	,819	-,121	241	,904	-,025	,207	-,433	,383
If my Partner or manager asks me to bend the IT security rules, I will do so.	,767	,382	-2,320	244	,021	-,481	,207	-,890	-,073
If I notice a colleague not following the IT security guidelines, I will address this with him/her.	,001	,974	1,264	241	,207	,238	,188	-,133	,608
I have stored or transported documents (that could be considered to contain sensitive/confidential information) on portable storage like a	,254	,615	-1,636	241	,103	-,402	,246	-,887	,082

Table 7. Equality of variances and means.

From these analysis it appears that “National culture”, tested as ‘Country of origin’, is a significant factor of influence in non-compliance behavior. More specifically, our study showed significant impact on the questions:

- Please rate your familiarity with the security policies for your organization.
- I sometimes need to bend the rules in order to get work done.
- If the IT security rules make no sense to me, I sometimes ignore them.
- If my manager asks me to bend the IT security rules, I will do so.

Further analysis

Question: *Please rate your familiarity with the security policies for your organization.*

Of the Dutch respondents, 73,4% state that they are Somewhat to Very Familiar with the existing security policies. For the Belgians, this is significantly (p=.000) lower: 54,1%.

Question: *Do you practice the IT security policies of your organization?*

There is a difference between familiarity with policy between The Netherlands and Belgium. And since there is some (albeit not statistical significant) homogeneity between awareness and practicing policy, differences are expected here as well. Of the Dutch respondents, 73,4% Sometimes to Always practice the policies. For the Belgians, this is 69,7%. However when correlation is measured over all possible answers (p=.283) or between the Sometimes to Always answers (p=.441) one finds no significant difference between Belgians and Dutch respondents.

No significant difference between the responses of both countries (p=.771) was found but when looking at the percentages, it is noticeable that in both countries, over ¼ of respondents are unaware of such policies although these types of software have been found to pose great risk of (accidentally) exposing sensitive data.

Question: *I sometimes need to bend the rules in order to get work done.*

A significant difference (p=.009) was found between Dutch and Belgian respondents. 60% of Belgians somewhat to strongly disagree with the statement against 50% of Dutch.

Question: *I sometimes need to share my passwords with colleagues so they can assist me with my tasks.*

No significant difference was found between Belgians and Dutch (p=.777). When looking at the statement itself, it quite clearly shows that sharing passwords is no necessity for the respondents: 86% do not agree with this statement, about half of which strongly disagree with the statement.

Question: *If the IT security rules make no sense to me, I sometimes ignore them.*

As predicted from the Hofstede cultural dimensions, there is a significant difference between The Netherlands and Belgium (p=.008). As the Latin culture (Belgium) has a higher Power Distance Index (PDI), they generally will be more likely to 'do as they are told'. However making autonomous decisions is also associated with Individuality (IDV) which is about equal for both countries.

Question: *I use Google Docs or other on-line collaboration software to store or share work with colleagues.*

With a p=.807 between The Netherlands and Belgium, there is no difference among them. Also, when looking at the frequencies, online collaboration outside of the enterprise network is not something the security manager should worry about.

Question: *I sometimes send documents (that could be considered to contain sensitive / confidential information) to a home/private email account so I can work from home.*

There is no difference between the Dutch and the Belgians (p=.904). When examining the frequencies, sending sensitive documents to home e-mail addresses is not something the security manager should worry about too much.

Question: *If my manager asks me to bend the IT security rules, I will do so.*

As predicted from the Hofstede cultural dimensions, there is a significant difference between The Netherlands and Belgium (p=.021). As the Latin culture (Belgium) has a much higher Power

Distance Index, they generally will be more likely to accept authority and therefore 'do as they are asked'.

Question: *If I notice a colleague not following the IT security guidelines, I will address this with him/her.*

A different distribution among the answers was found, but no significant difference (p=.207) between both countries. This is not really surprising as both countries about score equal in Hofstede's Individualism Index. Countries with higher PDI are less likely to address such issues with an equal, which can explain the difference in the 'never' and 'always' scores. There is no significant difference between Dutch and Belgian females (p=.310) or Dutch and Belgian males (p=.717).

Question: *I store or transport documents (that could be considered to contain sensitive/confidential information) on portable storage like a USB stick (excluding company issued encrypted devices).*

More Belgians than Dutch admit transporting data on unsecured USB sticks, but the difference is not significant at a 95% confidence level (p=.103). In percentages the responses show that 30.3% of the Dutch occasionally to always (answers 4 – 7) transport data on USB sticks, against 40.5% of the Belgians.

Summary of findings

The study learned us that:

- The Dutch are more likely to ignore rules if they make no sense to them. Explaining why the rules are there and what can happen if they are ignored is of importance.
- If a Partner or manager asks a Belgian employee to bend the IT security rules, he/she will more likely do so than a Dutch employee. As the Netherlands has a relatively low, and Belgium a moderately high PDI, this is not unexpected. It is therefore essential to have management buy-in in awareness programs and they should lead by example.
- In both countries roughly a third of the employees 'occasionally' to 'always' transport data on USB sticks. This may be related to the awareness of security policies and risk.
- Also the question related to correcting colleagues on security matters, didn't show a significant difference between the two countries. Based on their equal level of Individualism, this was also expected..
- When looking at the survey question related to masculinity, one sees little difference between the Dutch and the Belgian cultures, although the Belgians are more masculine and the Dutch are more feminine oriented.
- The Netherlands has have a very low UAI compared to Belgium, which has a high UAI value compared to the Netherlands and to the European average. Our study confirms that companies in low UAI countries may see their company rules and policies challenged or broken by employees, for pragmatic reasons.

CONCLUSION AND LIMITATIONS

This paper reported a study into the influence of national culture on non-compliance behavior in organizations. The literature review gave indications for a clear influence of national culture on compliance with IT Security rules and guidelines. Based on a survey study amongst employees of a big-5 accountancy firm in the Netherlands and Belgium, the influence of national culture was confirmed. Four out of ten non-compliance behavior statements in our study showed a significant difference between the two countries/national cultures. More specifically, our study showed significant impact on the questions:

- Please rate your familiarity with the security policies for your organization.
- I sometimes need to bend the rules in order to get work done.
- If the IT security rules make no sense to me, I sometimes ignore them.
- If my manager asks me to bend the IT security rules, I will do so.

In the country with the low PDI and UAI scores, the Netherlands, the employees seem to be more willing to 'bend the rules' or to 'disobey orders' of their superior, if their personal judgment tells them so.

However, we should also point out the limiting factors of our study. First, the small sample size has most likely influenced the survey outcomes. Where 653 results were needed to get a reliable representation of the population, the survey only delivered 246 results. The significance of the outcomes has to be viewed within this limiting perspective. Secondly, a third territory to research would have benefited the outcomes, particular those relating to cultural differences. Unfortunately this was not possible. Finally, as stated earlier in this paper, IT security is a vast area to explore and test, and has many links with behavioral sciences. This paper has limited itself to only one of the influencing factors found in current publications and research. This list is in no way comprehensive. The conclusions drawn from the outcomes have to be viewed within this limiting perspective.

REFERENCES

Al Awadi, M. and Renaud, K. (2007). Success Factors in Information Security Implementation in Organisations , IADIS International Conference e-Society 2007. Lisbon, Portugal. 3-6 July 2007

Babbie, E. (2003). Survey Research Methods, 3rd Edition, Belmont, California., Wadsworth Pub. Co. USA

Batenburg, R. (2007), E-procurement adoption by European Firms: A quantative analysis, Journal of Purchasing & Supply Management, 13, 182-192.

Birgelen, M. van, Ruyter, K.D, Jong, A.D., and Wtzels, M. (2002). Customer evaluations of after-sale service contact modes: An empirical analysis of national culture's consequences. International Journal of Research in Marketing, 19, 43-64.

Björck, J. and Jiang, K. (2006). Information Security and National Culture, MSc thesis, KTH Royal Institute of Technology, Stockholm, Sweden

Bond, M.H. (1984), Hofstede's Culture Dimensions ; An Independent Validation Using Rokeach's Value Survey, Journal of Cross-Cultural Psychology, Vol. 15, No. 4, 417-433.

Brooke, P. (2004). From the Top: Security Governance: Balancing Your Organization's Goals and Risk, Ensure well-directed security investments., American Financial Group publication, April 15, 2004, available from <http://nwc.securitypipeline.com>

Burke, B. and Christiansen, C. (2009). Insider Risk Management: A Framework Approach to Internal Security, RSA whitepaper based on IDC's 2008 Enterprise Security Survey, available from < http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf>

Chaula, J. (2006). A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance, PhD thesis, Stockholm University, Stockholm

Collins, J. (2001), Good to Great; Why some companies make the leap… and others don't, HarperCollins Publishers Inc, New York, NY

Cumps, B., Martens, D., De Backer, M., Haesen, R.,Viaene, S., Dedene, G., Baesens, B. and Snoeck, M. (2007). Predicting Business/ICT Alignment with AntMiner+, Katholieke Universiteit Leuven. KUL. Faculty of Business and Economics

Desisto,R., Plummer, D., and Smith, D. (2008). Tutorial for Understanding the Relationship Between Cloud Computing and SaaS, Gartner Research Paper, Available from http://www.gartner.com/resources/156100/156152/tutorial_for_understanding_t_156152.pdf

Ernst & Young (2009). Outpacing change: Ernst & Young's 12th annual global information security survey, Available from http://www.ey.com/Publication/vwLUAssets/Global_Information_Security_Survey_2009_ENG/$File/Global%20Information%20Security%20Survey%202009%20EN.pdf

Fallows, D. (2005), How Woman and Men Use the Internet, Pew Internet & American Life Project, report available from <http://www.pewinternet.org>

Gage, D. (2009). Somber year for RSA, Conference on cyber security, San Francisco Chronicle

Gefen, D., and Straub, D. W. "Gender Differences in Perception and Adoption of E-Mail: An Extension to the Technology Acceptance Model," MIS Quarterly (21:4), 1997, pp. 389-400.

Gordon, L., Loeb, M. and Lucyshyn, W. (2005). Computer crime and Security Survey, Computer Security Institute/FBI San Francisco Bureau, available from <http://www.gocsi.com or www.fbi.gov>

Harris Interactive for Websense Inc. 2006, Web@Work Survey 2006, Report available from <http://www.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork/IT_Decision_Makers.pdf>

Hofstede, G. (1980). Culture's consequences : international differences in work-related values, Beverly Hills, Sage Publications.

Hofstede, G. (1991) Cultures and organizations: software of the mind. Intercultural cooperation and its importance for survival. London: McGraw-Hill International (UK), Ltd.

Hofstede, G. (2000), The information age across cultures, paper presented at the 5th AIM conference – Information Systems and Organizational Change, proceedings CD-Rom, 10pp.

Hofstede, G. (2008), retrieved from http://www.geert-hofstede.com/hofstede_dimensions.php on February 28th, 2008.

Hung T., Ching, R. and Ja-Shen, C. (2007). Performance Effects of IT Capability and Customer Service: The Moderating Role of Service Process Innovation, International Conference on Wireless Communications, Networking and Mobile Computing.

Krom, E. (2006). Briefing Veiligheidsbewustzijn, Defensie Telematica Organisatie, available from http://www.isaca.nl/index.php?download=Briefing_Veiligheidsbewustzijn.swf

Leidner D. E., Carlsson S., Elam J. and Corrales, M. (1999), Mexican and Swedish managers' perceptions of the impact of EIS on organizational intelligence, decision making, and structure, Decision Sciences, 30 (3), 633-658.

Livonen, M., Sonnenwald, D. H., Parma, M., and Poole-Kober, E. (1998), Analyzing and understanding cultural differences: Experiences from education in library and information studies, paper presented at the 64th IFLA General Conference, Amsterdam, Netherlands.

Lutchen, M. (2004). Managing IT as a business : a survival guide for CEOs., Hoboken, N.J., J. Wiley.

Mathieson, K. (1991). Predicting user intentions:comparing the technology acceptance model with the theory of planned behaviour, Information System Research, Vol. 3 No. 2

Miller, S., Batenburg, R.S. & Wijngaert, L. van de (2006). 'National Culture Influences on European ERP Adoption.' In J. Ljungberg & M. Andersson (Eds.), 14th European Conference on Information Systems (pp. 1-12). Göteborg.

Mooij, de, M. (2000), The future is predictable for international marketers: Converging incomes lead to diverging consumer behavior', International Marketing Review, 17 (2)

Moreau, D. (2007). Aligning IT Security and Operations: Four Ways to Close the Gap, ConfigureSoft whitepaper, available from <http://www.configuresoft.com/ downloads.aspx>

Nath R, and Sadhu, K. (1998), Comparative Analysis. Conclusions, and Future Directions, in Comparative Management -A Regional View, Cambridge MA: Ballinger Publishing Company

Odubiyi, J. (2006) Develop your organisation's power Distance Index to attract and retain employees, EzineArticles.com, available from URL:http://ezinearticles.com/?Develop-Your-Organizations-Power-Distance-Index-to-Attract-and-Retain-Employees&id=389405

Png, I.P.L., Tan, B.C.Y. and Wee, K.L. (2001), Dimensions of national culture and corporate adoption of IT Infrastructure, IEEE Transactions on Engineering Management, 48 (1), 36-45.

Ponemon Institute (2007). Data Security Policies Are Not Enforced, US Survey of IT Practitioners, Research Report December 4, Available from http://www.redcannon.com/documents/RedCannonPonemonReport.pdf

Ponemon Institute (2006). National Survey On Managing The Insider Threat, Research Report, September 25, Available from http://www.arcsight.com

Raden, N. (2005). Shadow IT: A Lesson for BI, October edition, BI Review Magazine, Data Management Review and SourceMedia, Inc.

Richards, K. (2008). The Future of Information Security: 2008 and Beyond, Available from: http://www.cio.com/article/168352/The_Future_of_Information_Security_2008_and_Beyond

Robbins, R. (2005) The Nature of Personality: Genes, Culture, and National Character. Science, Vol.310. no.5745, pp.62-63

RSA (2007). The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk, Available from: http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf

Rundmo, T., Oltedal, S., Moen, B. and Klempe, H. (2004). Explaining risk perception. An evaluation of cultural theory, Norwegian University of Science and Technology, Trondheim

Schaffner, M. (2007). IT Needs To Become More Like "Shadow IT", Available from http://www.typepad.com

Schwartz, S.H. (1994), Beyond individualism-collectivism: New cultural dimension of values, in U. Kim, H.C. Tirandis, C. Kagitcibasi, S-C. Choi, and G. Yoon (Eds.), *Individualism and collectivism: Theory, method, and applications* (pp85-199). New York: Reidel.

Sherman, R. (2004) Shedding light on Shadow Systems, DM Direct, Athena IT Solutions

Siponen, M. (2000). A conceptual foundation for organizational information security awareness, Information Management &Computer Security 8/1 [2000] 31±41, MCB University Press

Slay, J. (2003), 'IS security, trust and culture: a theoretical framework for managing IS security in multicultural settings', The Emerald Research Register 20(3): 98-104.

Smith, P.B. and Bond, M.H. (1998) Social Psychology across Cultures. Paris: Prentice Hall Europe.

Sørnes, J-O., Stephens, K., Sætre, A.S. and Browning, L.D. (2004), The Reflexivity between ICTs and Business Culture: Applying Hofstede's Theory to Compare Norway and the United States, *Informing Science Journal*, Volume 7, 2004

Spafford, G. (2004). The Dangers that Lurk Behind Shadow IT, February 4, Available from http://www.earthweb.com

Straub, D. W. (1994), The effect of culture on IT diffusion: e-mail and fax in Japan and the US. Information Systems Research, 5 (1), 23-47.

Symantec (2009). 2009 Managed Security in the Enterprise Report, available from http://www.symantec.com/content/en/us/about/media/managed_security_ent_US_12Mar09.pdf

Van Decrean, J., (2007), Interculturele verschillen tussen internetsites van muziekwinkels uit Duitsland en de Verenigde Staten (in Dutch), Thesis University of Hasselt, Belgium.

Veiga, J., Floyd, S., and Dechant, K. (2001). Toward modelling the effects of national culture on IT implementation and acceptance , Journal of Information Technology, 16 (3)3, 145-158.

Verizon Business RISK (2009). 2009 Data Breach Investigations Report, Available from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Waarts, E., and Everdingen, Y. van, (2005), The Influence of National Culture on the Adoption Status of Innovations: An Empirical Study of Firms Across Europe, European Management Journal, Volume 23, Issue 6, December 2005, Pages 601-610.

Whitty, M. (2006). Report Surf Control: Trust and Risk in the Workplace, Queen's University, Belfast

Witty, R. and Wagner, R. (2005). Awareness Training Is Necessary to Support Your Information Security Program, Gartner Research, 31 January 2005, Available from http://www.gartner.com/resources/125800/125896/awareness_training_is_necess_125896.pdf

Witty, R., Girard, J., Graff, J., Hallawell, A., Hildreth, B., MacDonald, N., Malik, W., Pescatore,J., Reyanolds, M., Russell, K., Wheatman, V., Dubiel, J. and Weintraub, A. (2001). The Price of Information Security, Gartner Strategic Analysis Report, Available from http://www.gartner.com/DisplayDocument?ref=g_search&id=331017

Wold, G. (2004). Key factors in making Information Security Policies Effective, MSc thesis, Gjøvik University College, Norway

About the Authors

Taco Dols holds a Bachelor's degree in Business Administration and a Master's degree in Informatics. He has held positions at Gateway, Accenture and PricewaterhouseCoopers, and currently as Global Service Desk Manager at International Flavors & Fragrances Inc. Taco specializes in IT Service Desk Management and transforming organizations towards Service Desk model adoption. He performed the study reported in this paper as completion of his Master of Informatics study at Utrecht University of Applied Sciences.

A.J.Gilbert Silvius (1963) is Professor of Business, ICT and Innovation at Utrecht University of Applied Sciences. Gilbert has over 20 years experience as a consultant in the area of business and IT. He joined Utrecht University in 2003 and has since published on IT business value, Business IT Alignment and Project Management.