Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2012 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-1-2012

Factors influencing Non-Compliance behavior towards Information Security Policies

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

Taco Dols
HU University of Applied Sciences Utrecht, taco.dols@consultingency.com

Follow this and additional works at: http://aisel.aisnet.org/confirm2012

Recommended Citation
Silvius, A.J. Gilbert and Dols, Taco, "Factors influencing Non-Compliance behavior towards Information Security Policies" (2012). *CONF-IRM 2012 Proceedings.* Paper 39.
http://aisel.aisnet.org/confirm2012/39

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Factors influencing Non-Compliance behavior towards Information Security Policies

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

Taco Dols
HU University of Applied Sciences Utrecht
taco.dols@consultingency.com

Abstract
IT organizations and CEO's are, and should be, concerned these days about the (lack of) data confidentiality and the usage of 'shadow' IT systems by employees. Not only does the company risk monetary loss or public embarrassment, the senior management might also risk personal fines or even imprisonment. Several trends reinforce the attention for these subjects, including the fact that an increasing number of people perform parts of their work tasks from home (RSA, 2007) and the increasing bandwidth available to internet users which makes them rely on the Internet for satisfying their business and personal computing needs (Desisto et al. 2008). Employee compliance with the existing IT security policies is therefore essential.
This paper presents a study on factors that influence non-compliance behavior of employees in organizations. The factors found in literature are tested in a survey study amongst employees of a big-four accountancy firm in the Netherlands and Belgium. The study concludes that stricter IT governance and cultural aspects are the most important factors influencing non-compliance behavior.

Keywords
Information Systems Security, Non-Compliance, Culture, IT Governance.

1. Introduction
Information security is a widely discussed topic (e.g., Brooke, 2004; Gordon, 2005; Ponemon Institute, 2007). Despite years of investments in security technology and processes, genuinely 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. This includes establishing meticulous risk fundamentals and requires 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 and iPads, increase the number of possibilities for sensitive information falling in the wrong hands. To make matters worse, some companies are decreasing budgets in information technology (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 survey of 1000 IT managers in the U.S. and Europe in January 2009, 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). Some argue that careless and negligent employees pose the greatest security threat to a company (Ponemon Institute, 2006; Moreau, 2007; Whitty, 2006; Krom, 2006).
This study aims to identify the factors that influence non-compliancy behavior of insiders (employees). For example the carelessness with which employees approach data security and the usage of 'shadow' IT systems like USB memory devices.
After a literature review on the factors influencing non-compliance behavior, the factors derived from literature are tested in a survey study amongst employees of a big-four accountancy firm in the Netherlands and Belgium. The results of this are analyzed for the relationships between the influencing factors of non-compliance behavior and the behavioral aspects of non-compliance. The final section of the paper presents the conclusions drawn from the study.

2. Factors influencing Non-Compliance behavior

Several studies have been conducted to find out what causes employees not to follow the IT security policies and guidelines (e.g. Moreau, 2007; Lutchen, 2004; Ponemon Institute, 2007; Cumps et al., 2007). Often employees are unaware of the existence of security policies or do not see the relationship between the policy and their daily tasks and see it more as a nuisance (Höne and Eloff, 2002). A possible link with IT governance has also been suggested (Moreau, 2007). 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). Our study focuses on the human risk factors.
A review of the existing literature resulted in a selection of five commonly mentionned influencing factors: Carelessness; Lack of Awareness; Stricter IT Governance; Poor Business – IT Alignment; Culture. Table 1 shows these factors and their source.
The following section discusses the factors in more detail.

Carelessness

A survey (Ponemon Institute, 2007) among 893 IT professionals in the USA showed that they consider malicious or negligent insiders (employees) to pose the greatest threat to an organization's information assets. For example, despite the existence of policy forbidding its use, over half of respondents admit they have transferred confidential data onto a USB memory stick.

Another survey (RSA, 2007) among government and corporate employees in two US cities confirmed that the biggest threats in a workplace are "often unintentional, often resulting from carelessness or ignorance of individuals within the organization or company". Carelessness and ignorance can be the result of an incorrect assessment of the risk involved. It is therefore related to lack of knowledge.

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)
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.

Lack of Awareness

Mathieson (1991) states that 'Information Systems can only be useful if people use them' and the same can be said for information security guidelines. Therefore, information security awareness is of the highest importance, as the defined guidelines and procedures can be misinterpreted or not practiced by end-users, which results in losing their usefulness (Straub and Welke, 1998).

Increasing awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. And although research has shown that end-users think giving security awareness training to be one of the least-effective approaches to manage IT risk, businesses with such training programs in place have shown to have reduced levels of risk (Witty and Wagner, 2005). The National Institute of Standards and Technology (NIST) confirms that awareness can be created through education: Explaining what happens to an organization, its mission, customers, and employees if security fails, motivates people to take security seriously (NIST, 1995).

Strict IT Governance

In the research, IT Governance has been tested as a driver for non-compliant behavior towards IT Security. IT Governance includes activities such as control of the work performed by IT professionals, compliance with internal policies or regulations, justification of IT spending, accountability, transparency and overall connecting with the needs of customers, the broader organization, and other stakeholders. Making sure that IT investments are in sync with the organization's business objectives proves to be "more challenging than initially expected, especially in today's fast-changing, dynamic environment" (Cumps et al., 2007). This is because historically, from a business point of

view, IT has been one of the least understood expenditures and also one of the most poorly managed. As IT managers have often failed to weigh IT business risk against cost, this has resulted in increased expenditure and reduced ability to leverage the investment portfolio value (Lutchen, 2004).

Poor Business-IT Alignment

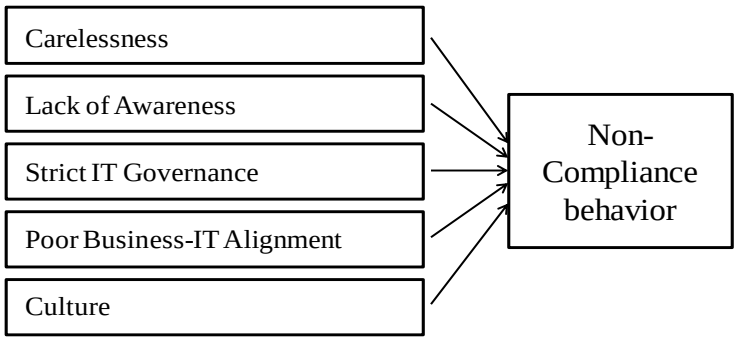

Figure 1. Conceptual model of the study.

The problems of aligning IT to Business objectives is a widely discussed topic (for example Spafford, 2004; Raden, 2005; Cumps et al., 2007). Enablers and inhibitors of alignment are explored by Luftman and Brier (1999). Raden (2005) states that non-compliance behavior results from a number of factors, including lack of business-IT alignment, Also Booz Allen Hamilton (2004) relate non-compliance to business-IT alignment. This consultant company identifies non-compliance behavior as performing IT functions outside the formal IT organization. They state "The problem here is … the inadequacies in the normal service delivery model that prompted the business unit to circumvent it." This also points to lack of business-IT alignment.

Culture

National cultural different attitudes towards the perception of risk have been identified as one of those human risk factors (Rundmo et al., 2004). National culture is much more dominant than the organizational culture of a company (Hofstede, 2001). Research has not often established a connection between cultural dimensions and information security. Björck and Jiang (2006) in their study "Information Security and National Culture" make a first attempt in this direction (albeit for software implementation of an ERP system) and Al-Awadi and Renaud (2007) establish a link between trust (in IT) and culture. According to Gartner (Witty et al., 2001) trust "…trust results from the effective application of information security techniques."

3. Research design

The empirical part of our study was aimed at discovering to which degree the factors derived from literature correlated with non-compliance behavior. The conceptual model for this study can be depicted as shown in Figure 1. However, further conceptualization of the identified factors is required to study their influence on non-compliance behavior.

In order to test the factors, a survey study was designed that consisted of 21 questions. In the survey, the factors influencing non-compliance behavior were tested in nine questions. The questions were largely posed as statements to which the respondents could agree or disagree.

The factor *Carelessness* was not tested specifically, because the potential questions would be very similar to the questions testing actual non-compliant behavior.

The factor *Lack of Awareness* was tested with the questions:

Please rate your familiarity with the security policies for your organization.

I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)

This last question is relevant because the organization has specific policies concerning the use of these platforms, but these policies are not labeled "security".

The factor *Strict IT Governance* was tested in the questions:

Compared with previous years, I find that IT security policies have become stricter.

I sometimes feel that IT security prevents me to work efficiently.

Another factor is *Lack of Business-IT Alignment*. This factor was tested with the questions:

My IT department provides me with the technology I need to perform my tasks.

I sometimes feel that less budget is available for IT (projects) than before.

I should be able to install the applications I need on my work computer.

The factor *Culture* was tested with the questions:

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

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

These questions may seem to represent already non-compliance behavior. However, in the question regarding the factors, we specifically address external influences on the behavior of the respondent, where as a test of non-compliance, the questions address actual behavior.

To test whether the respondent actually showed non-compliance behavior, we asked seven questions. These questions included the usage of unauthorized (shadow) IT systems, like Google Docs, and unwanted behavior such as sharing and storing company data on unsecured devices like USB drives. Again, the questions were posed as statements to which the respondents could agree or disagree. The specific questions were:

Do you practice the IT security policies of your organization?

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

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

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

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

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.

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).

All of these questions portray specific behavior that is not compliant with company policies on IT security.
Another five general descriptive questions were asked about the respondent and his/her working environment. The design of the total questionnaire is shown in table 2.
The survey was conducted amongst employees of one of the big-four accounting firms in The Netherlands and in Belgium between December 2008 and February 2009. 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 an Internet connection to a web-page from NetQuestionnaires (Computerized Self-Administered Questionnaire, Babbie 2003). They have been invited trough an intercompany Lotus Notes email with a hyperlink.

	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 derived from the factors influencing non-compliance behavior			
6	Do you practice the IT security policies of your organization?	7-step semantic differential	Never to Always
7	Please rate your familiarity with the security policies for your organization.	7-step semantic differential	Very Unfamiliar to Very Familiar
8	I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)	7-step semantic differential	Strongly Disagree to Strongly Agree
9	Compared with previous years, I find that IT security policies have become more strict.	7-step semantic differential	Strongly Disagree to Strongly Agree
10	I sometimes feel that IT security prevents me to work efficiently.	7-step semantic differential	Strongly Disagree to Strongly Agree
11	My IT department provides me with the technology I need to perform my tasks.	7-step semantic differential	Strongly Disagree to Strongly Agree
12	I sometimes feel that less budget is available for IT (projects) than before.	7-step semantic differential	Strongly Disagree to Strongly Agree
13	I should be able to install the applications I need on my work computer.	7-step semantic differential	Strongly Disagree to Strongly Agree
14	If my manager asks me to bend the IT security rules, I will do so.	7-step semantic differential	Strongly Disagree to Strongly Agree
15	If I notice a colleague not following the IT security guidelines, I will address this with him/her.	7-step semantic differential	Strongly Disagree to Strongly Agree
Questions to test non-compliance behavior.			
16	I sometimes need to bend the rules in order to get work done.	7-step semantic differential	Strongly Disagree to Strongly Agree
17	I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	7-step semantic differential	Strongly Disagree to Strongly Agree
18	If the IT security rules make no sense to me, I sometimes ignore them.	7-step semantic differential	Strongly Disagree to Strongly Agree
19	I use Google Docs or other on-line collaboration software to store or share work with colleagues.	7-step semantic differential	Never to Often
20	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 Disagree to Strongly Agree
21	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	Never to Often

Table 2. Design of the questionnaire

In total 273 surveys were completed (139 for the Netherlands, 134 for Belgium), corresponding with a response rate of 42.1% (38.6% for the Netherlands, 46.4% for Belgium). Table 3 provides the descriptive statistics of the respondents.

Question		Values	Response [%]
1	Gender	[Male]	55
		[Female]	45
2	Country of origin	[Belgium]	49
		[the Netherlands]	51
3	Age group	[18-23]	8.8
		[24-29]	42.9
		[30-35]	23.8
		[36-41]	9.2
		[41+]	15.4
4	Company laptop	[Yes]	93
		[No]	7
5	Number of years with the company	[<1 yr]	19.8
		[1-3 yr]	32.2
		[4-6 yr]	15.8
		[>6 yr]	32.2

Table 3. Descriptive statistics of the respondents

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

4. Findings

As a first result, the mean scores on the questions are shown in table 4. These results show that the respondents are reasonably familiar with the IT security policies and generally comply with them. However, the scores on “I sometimes need to bend the rules in order to get work done.” and “If my manager asks me to bend the IT security rules, I will do so.” also suggest that these policies are not followed all the time, resulting in non-compliance behavior. The correlation between the factors that influence non-compliance behavior and the questions that show non-compliance behavior is shown in table 5.

	Question	Values	Scale	Response Mean
Questions derived from the factors influencing non-compliance behavior				
6	Do you practice the IT security policies of your organization?	Never to Always	1 to 7	5,1
7	Please rate your familiarity with the security policies for your organization.	Very Unfamiliar to Very Familiar	1 to 7	4,7
8	I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)	Strongly Disagree to Strongly Agree	1 to 7	4,9
9	Compared with previous years, I find that IT security policies have become more strict.	Strongly Disagree to Strongly Agree	1 to 7	4,6
10	I sometimes feel that IT security prevents me to work efficiently.	Strongly Disagree to Strongly Agree	1 to 7	3,6
11	My IT department provides me with the technology I need to perform my tasks.	Strongly Disagree to Strongly Agree	1 to 7	5,4
12	I sometimes feel that less budget is available for IT (projects) than before.	Strongly Disagree to Strongly Agree	1 to 7	3,6
13	I should be able to install the applications I need on my work computer.	Strongly Disagree to Strongly Agree	1 to 7	4,1
14	If my manager asks me to bend the IT security rules, I will do so.	Strongly Disagree to Strongly Agree	1 to 7	3,6
15	If I notice a colleague not following the IT security guidelines, I will address this with him/her.	Strongly Disagree to Strongly Agree	1 to 7	4,1
Questions to test non-compliance behavior.				
16	I sometimes need to bend the rules in order to get work done.	Strongly Disagree to Strongly Agree	1 to 7	3,3
17	I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	Strongly Disagree to Strongly Agree	1 to 7	2,3
18	If the IT security rules make no sense to me, I sometimes ignore them.	Strongly Disagree to Strongly Agree	1 to 7	3,4
19	I use Google Docs or other on-line collaboration software to store or share work with colleagues.	Never to Often	1 to 7	1,6
20	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.	Strongly Disagree to Strongly Agree	1 to 7	2,0
21	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).	Never to Often	1 to 7	2,9

Table 4. Mean scores

Questions derived from the factors influencing non-compliance behavior	*Questions to test non-compliance behavior.*						
	Do you practice the IT security policies of your organization?	I sometimes need to bend the rules in order to get work done.	I sometimes need to share my passwords with colleagues so they can assist me with my tasks.	If the IT security rules make no sense to me I sometimes ignore them.	I use Google Docs or other on-line collaboration software to store or share work with colleagues.	I sometimes send documents (that could be considered to contain sensitive/confident ia information) to a home/private email accou so I can work from home.	I store or transport documents (that could b considered to contain sensitive/confidential information) on portable storage like a USE stick (excluding company issued encrypted devices).
Please rate your familiarity with the security policies for your organization.	**,486(**)**	0,000	-0,119	-0,091	-0,067	-,128(*)	-0,092
I am aware of company policies concerning Instant Messaging usage (like MSN) and Peer to Peer software usage (like Kazaa, BitTorrent or Limewire)	**,253(**)**	-0,098	-0,042	-,196(**)	-0,058	-0,055	-0,110
Compared with previous years, I find that IT security policies have become more strict.	**,207(**)**	0,116	-0,009	0,058	0,037	-0,002	0,056
I sometimes feel that IT security prevents me to work efficiently.	,166(**)	**,498(**)**	-0,021	**,284(**)**	0,010	0,023	0,037
My IT department provides me with the technology I need to perform my tasks.	**,275(**)**	-,245(**)	-0,056	-0,112	-0,038	-0,055	-0,045
I sometimes feel that less budget is available for IT (projects) than before.	-0,083	0,121	0,073	0,063	0,120	0,030	-0,109
I should be able to install the applications I need on my work computer.	-0,102	0,114	0,012	**,230(**)**	0,086	0,084	,164(*)
If my manager asks me to bend the IT security rules, I will do so.	**,246(**)**	**,288(**)**	0,089	**,326(**)**	0,109	0,050	,157(*)
If I notice a colleague not following the IT security guidelines, I will address this with him/her.	**,245(**)**	0,021	-0,031	-,149(*)	0,036	-0,082	0,060

(**) = Correlation is significant a (**) = Correlation is significant at the 0.01 level (2-tailed)
(*) = Correlation is significant at (*) = Correlation is significant at the 0.05 level (2-tailed)

Table 5. Correlations between factors that influence non-compliance behavior and actual non-compliant behavior

From these scores it shows that the factors most influencing non-compliance behavior are:

- *Familiarity with the security policies of the organization*.
- *The feeling that IT security prevents efficient working*.
- *The influence of the manager*.

And although the correlations found are not particularly strong, they do are significant.

The types of non-compliance behavior that are most impacted are:

- *The practicing of IT security policies*.
- *Bending the rules to get work done*.
- *The sense of IT security roles*.

5. Analysis

In this section, the most influential factors are discussed.

Familiarity with the security policies of the organization.

This factor correlates significantly and moderately strong with the practicing of IT security policies. This relationship is in line with the results of Witty and Wagner (2005) and RSA (2007) that show that lack of awareness relates to non-compliance.

The feeling that IT security prevents efficient working.

This factor, resulting from strict IT governance policies, correlates moderately strong with the feeling that sometimes rules need to be bend. Again this is a logical and expected result. A somewhat weaker correlation was found with the ignoring IT security policies. Since this factor represents aspects of frustration, and the effect that has on non-compliance, it may illustrates the need of effective communication of the how and why of IT security policies.

The influence of the manager.

This factor correlates significantly with a several aspects of non-compliant behavior. It illustrates the exemplary role of the manager in compliance.

Although the results shown above are not unexpected, it is remarkable that there is no noteworthy correlation between the factors influencing non-compliance behavior and the questions concerning the use of Google Docs, unsecured USB sticks, emailing to home, etc. It seems almost as if these more modern ways of non-compliance behavior are not considered security risks at all.

When the results from the survey are analyzed to the five descriptive questions, it shows that the 'Country of origin' and 'Company laptop' ownership have a strong impact both on the scores on the factors that influence non-compliance behavior as on the questions that show non compliance behavior. Regarding the ownership of a company laptop this confirms the conclusion of Whitty (2006) that mobile users are more likely to take more risks with the usage of uncontrolled data flows.

Regarding the impact of country of origin, a potential explanation could be that IT security policies are better known in the Dutch company than in the Belgium company. However, this explanation does not account for all the correlations found. A more plausible explanation therefore could be the influence of national culture on the culture of the local organizations in Belgium and the Netherlands and the resulting attitude towards risk, authority and compliancy of the respondents. Also regarding this aspect, the study of Whitty (2006) on "Trust and Risk in the Workplace" showed significant differences per country.

6. Conclusions and Limitations

This paper presented a study on factors influencing non-compliance behavior in organizations by insiders or employees. Based on literature, five factors were identified: Carelessness; Lack of Awareness; Stricter IT Governance; Poor Business – IT Alignment; Culture. These factors were then tested in a survey study in Netherlands and Belgium. The study showed some significant impact of part of the influencing factors on certain non-compliance behavior, although on several factors, no influence was found. The influences are shown in figure 2.

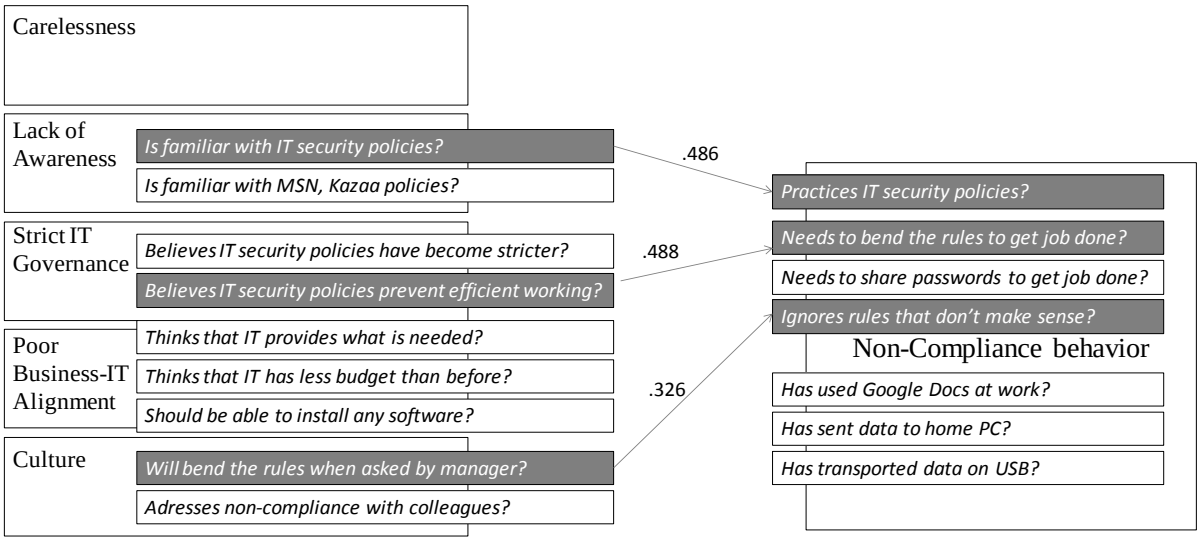

Figure 2. Strongest correlations between factors that influence non-compliance behavior and aspects of non compliance behavior (indicated in dark-grey)

The results of the study underline the need for adequate communication of the need, policy and risk, related to IT security.

Surprisingly, a significant correlation between the factors influencing non-compliance behavior and the use of Google Docs, unsecured USB drives, emailing to home, etc. is lacking. This may indicate that the awareness that these actions are in fact acts of non-compliancy, is not very high. The practical implication from these results is that organizations should continuously work on a creating improved awareness of IT security risks and policies.

Another conclusion from our study is that conscious non-compliant behavior (knowingly bend, break or ignore the IT rules) seems to occur when employees feel they are restricted in doing their work effectively as well as if they are told to do so by their manager. This conclusion underlines the need for adequate alignment of business and IT.

The results of our study also indicated that 'Country of Origin' may be a factor of influence in either awareness of security policies, or (non-)compliance behavior. We suggest that this influence is further explored in a follow-up study.

As limitation of the study, we want to put these conclusions in the context of the limiting factors encountered. 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 273 results. The significance of the outcomes has to be viewed within this limiting perspective. Secondly, 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

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

Booz Allen Hamilton (2004) Shining the Light on Shadow Staff, available from http://www.boozallen.com/media/file/Shining_Light_on_Shadow_Staff.pdf

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>

CBS (Central Bureau for Statistics) (2004) De Digitale Economie 2004, Centraal Bureau voor de Statistiek, Voorburg / Heerlen, Netherlands (in Dutch)

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

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

Deming, W (1986) Out of the Crisis, MIT Center for Advanced Engineering Study. ISBN 0-911379-01-0.

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>

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

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>

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

Hofstede, G (2001) Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations, Sage Publications, London, UK

Höne, K and Eloff, J (2002) What makes an Effective Information Security Policy?, Network Security, Volume 2002, Issue 6, June 2002.

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>

Luftman, J (1999) Assessing Business Alignment Maturity, Communications of AIS, Volume 4, Article 14 1

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

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

NIST Handbook, The (1995) An Introduction to Computer Security, NIST special publications 10-95)

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>
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>
Sherman, R. (2004) Shedding light on Shadow Systems, DM Direct, Athena IT Solutions
Spafford, G. (2004) The Dangers that Lurk Behind Shadow IT, February 4, Available from <http://www.earthweb.com>
Straub, D and Welke, R (1998) Coping with systems risk: security planning models for management decision making, MIS Quarterly, Vol. 22 No. 4
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>
Verizon Business RISK (2009) 2009 Data Breach Investigations Report, Available from <http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf>
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>