The organizational Relationship between Compliance and Information Security[1]

Maurizio Cavallari[2]
Università Cattolica del Sacro Cuore di Milano–Italy

ABSTRACT

Organizations continually experience losses, financial and otherwise, due to non-compliant behaviour (Stanton et al., 2005). As managers must balance the task of motivating employees to comply, without imposing counter-productive forms of punishment for non-compliant behaviour, executing leadership in agreement with IT security policy and compliance is emerging as a challenge (D'Arcy et al., 2009).

Information system security is an essential feature in most organizations today and compliance is one method of gaining visibility for processes and controls that ensure digital security, the organizational aspect of which being explicit in the Information Security Plan (ISP). The purpose of this paper is to investigate the perceptions and beliefs held by employees and managers regarding compliance with their company's ISP, by means of the identification of a set of constructs based on workplace culture, personal attitudes and the players (actors) involved. Fifteen variables have been used to build the constructs and this research, an empirical investigation of a set of 7 hypotheses, has been conducted by means of a questionnaire and presents the confirmation of these hypotheses, along with other significant findings, as its conclusions.

1 A preliminary, reduced, version of the paper appeared at the conference named "Workshop di Organizzazione Aziendale", held in Naples, Italy (2011).

2 The author also wishes to thank the anonymous reviewers of IJABW for the help in enhancing the overall quality of the paper

INTRODUCTION

Compliance is a conceptual area that focuses on satisfying, at a global level, the requirements of various laws and regulations and, at a local level, mandates and policy frameworks, the majority of which also have the purpose of improving security, including information security. This paper focuses on Compliance in relation to Information Security.

Compliance has a variety of definitions, all pertaining to regulations and laws in force, which also address audit matters in order to assess the implementation of those regulations; i.e. "[compliance is] either a state of being in accordance with established guidelines, specifications or legislation or the process of becoming so" (Techtarget 2010). Those regulations come primarily from legislation and secondly from best practices (Siponen 2005; Schlarman 2007); only at the latter level can an organization's own specific guidelines be derived from internal practices or experience, whereas legal rules are not negotiable.

Within each organization itself, the Information Security Plan is the major source of regulation, as it comprises both legal requirements and internal policies. As the result of both the exogenous and endogenous drive, organizations create an Information Security Plan (ISP) to provide employees with those guidelines (Whitman et al. 2001).

BRIEF ABOUT ISS

Information Systems Security (ISS) is the name given to all processes and activities aimed at protecting electronic information from tampering, corruption, theft, and/or unauthorized use or access. The prime objective of ISS is to make information available to its intended users for productive use (Whitman, 2008).

In the early information system years, it was believed that self-sufficiency and adhering to the best practices in ISS would suffice for information protection (Siponen and Vance, 2010). Over time, information sensitive sectors like healthcare, finance, and education developed policies to provide a systematic approach to the ISS process (Dhillon, 1997; Thomson and von Solms, 1998; Siponen, 2005).

Some research shows that increased security breaches during the last decade forced regulators to realize that conventional methods of securing digital information may no longer be applicable. This increase initiated the need for successful compliance programs that are proactive in avoiding the risks of security breaches (Doherty and Fulford, 2006), the incidence of which has been rising (Gordon et al., 2006; Ponemon, 2009a).

Other authors focus on the dual nature of Information Security (Spagnoletti and Resca, 2008) and consequently an organization's overall security strategy must integrate a sound compliance program that covers all departments and departmental activities (Neumann, 1999).

Decentralized approaches have been difficult to implement and monitor (Anderson, 2008) thus research findings show the need for a unified approach, where information trickles down to various levels of the organization, which is easy to monitor and whose benefits are quantifiable right from the beginning of implementation (Stallings, 2008, Bodungen et al., 2008).

OBJECTIVES AND SCOPE

The organizational relationship between Compliance rules (exogenous) and internal policies for ISP (endogenous) can be observed as a threefold conceptual definition: Workplace Culture, Personal Attitudes and Actors (Hu et al., 2007; Dinev and Hu, 2007; Elffers et al., 2003, Boss et al., 2009; Cavusoglu et al., 2004).

This paper aims to explore the impact of the organizational issues of compliance on an organization's existing information security policy on the basis of this threefold approach.

Regardless of where an organization is on the compliance/non-compliance spectrum (Elffers, 2003), the framework discussed in this paper has the potential of revealing those cracks, through which many important aspects of compliance may fall, the nature of non-compliant employees (Bulgurcu et al., 2010), and those aspects that jeopardize security (Melville et al., 2003).

The revelation of those aspects can help scholars with a stream of research findings and can also help managers put the organization on a track to compliance and a more desirable state of information systems security (Warkentin and Willison, 2009).

LITERATURE REVIEW

Extant literature suggests that most threats to an organization's information security arise from the careless and negligent attitudes and behaviour of employees (Siponen et al., 2009; Siponen and Vance, 2010; Dhillon, 2005; Im and Baskerville, 2005). When evaluating the behaviour of employees who choose either to comply or not to comply with information security policies and procedures, there are several pertinent issues to consider (Herath and Rao, 2009; Stanton, 2005).

According to Poneman's (2009) study of security policies and employee compliance behaviour, most of the attrition in complying with security policies occurs when the organization fails to provide adequate training to employees. This is a major drawback when companies invest enormous amounts of money in planning policies and deploying infrastructure and technologies but fail to train the human asset that actually executes the organization's plans and strategies through employee expertise and knowledge.

An important issue is about that personal attitude that denotes an individual employee's motivation towards complying with security policy (Staton et al., 2005; Myryy et al., 2009). These attitudes are also determined by his/her positive and/or negative feelings about the individual and organizational consequences of non-compliance.

If an employee is motivated and possesses the willingness and ability to carry out specific compliance behaviour, the chances are greater that he/she will actually execute that behaviour (Ajzen and Fishbein, 1980; Ajzen, 1991; Mathieson et al., 2001; Ajzen and Albarracin, 2007; Fishbein, 2007).

SUMMARY OF PREVIOUS FINDINGS AND CAUSES WITH RESPECT TO EXISTING LITERATURE

Finding	Causes	Authors
IS threats	IS threats	Siponen et al., 2009; Siponen and Vance, 2010; Dhillon, 2005; Im and Baskerville, 2005
Non compliance	Behaviors/ employees	Herath and Rao, 2009; Stanton, 2005
Attrition in complying with security policies	Organization fails to provide adequate training	Poneman, 2009
Motivation for security policy	Personal attitude	Staton et al., 2005; Myryy et al., 2009
Feelings about consequences of non-compliance	Motivation	Ajzen and Fishbein, 1980; Ajzen, 1991; Mathieson et al., 2001; Ajzen and Albarracin, 2007; Fishbein, 2007
Risk of security breaches	Negligent attitude	Lee and Lee, 2002; Boss and Kirsch, 2007
Attitudes are the result of favourable or unfavourable perceptions	Employee perceptions about the ISP	West, 2008, Warkentin and Willison, 2009
Policies being ineffective	No perception of actual plans	Spagnoletti et al., 2011
Ineffective policies and breaches	Employees overlook the security norms	Ponemon, 2009; Cavusoglu et al. 2004a
Organizations fail about security compliance as an enterprise wide	Policies and regulations are too complex to be understood	Staton et al., 2005
Management cannot enforce policies	Employees find ways to avoid penalties	D'Arcy, 2009; Dhillon, 1997

Delving a bit deeper into the threats arising from non-compliant behaviour, recent research suggests that it is mostly the negligent attitude of employees that places the organization in serious risk of security breaches (Lee and Lee, 2002; Boss and Kirsch, 2007). These attitudes are the result of favourable or unfavourable employee perceptions about ISP as a whole; favourable perceptions about ISP, have proven to lead to fewer instances of non-compliance (West, 2008, Warkentin and Willison, 2009).

A further relevant issue arises from policies that are ineffective, i.e. when organizations plan and record strategies on paper with no serious thought about their actual execution (Spagnoletti et al., 2011). This emerged as one reason why employees overlook the security norms and perform carelessly at times, leading to ineffective policies and breaches in compliance that go unreported (Ponemon, 2009; Cavusoglu et al. 2004a).

Other authors state that organizations fall short of making security compliance an Enterprise-wide campaign because rules, policies, and regulations are too complex to be understood by employees (Staton et al., 2005). Organizations often fail to enforce policies to protect information systems strictly enough and are much too lenient in executing and then governing the policies with which employees, who have by now become lax, must comply, thus adding to inefficiency, Employees often find ways to avoid penalties or punishment because policies are not stringent enough and management, therefore, cannot enforce them (D'Arcy, 2009; Dhillon, 1997).

It has been argued that most employees are generally unaware that policies pertaining to security and compliance within the organization even exist. (Boss et al., 2009; Bodungen, 2008). This failure to communicate policies to every channel of the organization at the outset constitutes an additional major hurdle for achieving information security capabilities through compliance (Spagnoletti et al.,2011).

For example, the U.S. Securities and Exchange Commission (SEC) failed to resolve twelve of the twenty information security weaknesses previously reported by the United States Government Accountability Office audit for the year 2008 (GAO, 2008). Despite the obvious impact of information security on the stability of the World's securities market and pressure from government and banks, if such a vital body as the SEC failed to implement its Information Security Program fully (ivi, pages 12–14), how can any other organization even imagine it will succeed in fully implementing ISPs?

THE RESEARCH QUESTIONS

Interesting findings about Compliance and ISP show that what plays a fundamental role is the perception of the "sense of security" (Anderson, 2009). This suggests that perception and personal reflections are far more important than actual levels of technical implementation.

Accordingly, the investigation of this research shifts from technical issues to Compliance behaviour (Ajzen, 1991), in order to understand the aspects pertaining the employees' perception of security and ISP (Åhlfeldt and Spagnoletti, 2007) and therefore its impact.

In the attempt to answer hidden and non-salient facets of Compliance and ISP (Ranbhotam and Mitra 2009), a series of four general Research Questions (R.Q.) guide the remainder of the discussion:

1. Is Compliance perceived as an essential component of organizational culture?
2. Is personal attitude playing a role in order to achieve Compliance?
3. What is the perception about the organizational actors who should enforce Compliance towards ISP?
4. Is there a difference between the points of view of employees and managers?

To be able to answer these R.Q.s we decided to take into account the perception of employees and managers about Compliance and ISP along with the personal ideas about what Compliance is about and who should enforce Compliance and ISP.

This decision about the R.Q.s is consistent with previous findings of existing literature and robust theoretical frameworks (Fishbein and Ajzen, 1975; Ajzen and Fishbein 1980; Ajzen and Albarracin, 2007; Myyry et al., 2009; Straub, 1998; West, 2008). A set of 7 hypothesis were built in order to respond to R.Q.s.

RESEARCH MODEL AND HYPOTHESIS

As discussed earlier, organizational aspects of Compliance with ISP consist of distinguishable dimensions of culture, attitudes and actors. The proposed research model is derived from various models by Ajzen, Fishbein, Siponen and Baskerville (see table 1).

To answer to the four R.Qs. mentioned above, three constructs were identified as instruments to use in order to guide the analytical results of the empirical investigation: Workplace Culture; Personal Attitude; Actors.

Table 1
Constructs and Sources

Construct	Sources
Workplace Culture	Boss and Kirsch, 2007; Boss et al., 2009; D'Arcy et al. 2009; Fishbein et al., 2007;
Attitude	Fishbein and Ajzen, 1975, Ajzen and Fishbein, 1980, Ajzen, 1991; Ajzen and Albarracin, 2007; Herat and Rao, 2009; Papadaki, 2010;
Actor	Bulgurcu et al. 2010; Dinev and Hu, 2007; Freeman, 2007; Im and Baskerville, 2005; Myyry et al., 2009; Siponen and Vance, 2010; Siponen et al., 2009.

To answer to the four R.Q. mentioned above, three constructs were identified as instruments to use in order to guide the analytical results of the empirical investigation: Workplace Culture; Personal Attitude; Actors.

Construct WPC

From a socio-technical standpoint, the workplace culture (WPC) was investigated according to aspects related to the employees' belief that information security is desirable and the perception that Compliance can enforce security. If security is the desirable goal and Compliance is perceived throughout the organisation as the tool to achieve the desired goal, this could prove to be a positive motivation within workplace culture.

The construct also accounts for the perception of punishment for non-compliance and the perception of IS threats as the antecedents for Compliance (Dhillon and Beckhouse, 2001). The construct serves also to verify whether Compliance is seen as a rewarded and organization-wide cultural force to be pursued by everyone (Boss and Kirsch, 2007). Literature has so far demonstrated the interdependency between beliefs, as antecedent, and behaviour, as consequent (Fishbein, 2007).

Construct ATT

The personal attitudes (ATT) of employees are defined according to the Theory of Planned Behavior (Fishbein and Ajzen, 1975; Ajzen and Fishbein, 1980; Ajzen 1991), which makes the distinction between technological driven aspect and behavioural aspects driven by attitude. IT leadership occurs when, in order to oblige processes to follow certain paths and steps, there is the side effect to make those behaviours complaint with the Information Security Plan (Vardi and Weitz, 2004). This is a major drawback, for instance, of ERP implementation. Attitude driven behaviour is influenced directly by individual beliefs as well as IT constraints. IT leadership is particularly effective when processes are loosely structured and there is a strong need for compliance.

Construct ACT

The Actors (ACT) construct was built in order to understand the perception of those individuals within the organization who are believed to be the most important in the enforcement of Compliance with ISP. Complete understanding of ISP can be difficult to achieve and might vary according to the position of the individual in the organization, i.e. managers and employees. Misunderstanding or ignorance of ISP naturally leads to non-compliance and a more vulnerable information system (Freeman, 2007; Im and Baskerville, 2005). The effect of the behaviour of other actors was also investigated according to the effort required for compliant behaviour and the perception of employees about the conditions implemented to facilitate counter-balancing the reduction in productivity associated with Compliance (Siponen and Vance 2010; Warkentin et al. 2004). Perception, according to the position in the organization of the individual, about who is the actor can also influence behaviour (Siponen et al. 2009).

The following hypothesis were formulated for the empirical investigation:

- H1: Rewards for compliance with the ISP are positively perceived as beneficial.
- H2: There is positive relation between organisational culture and personal attitudes.
- H3: There is an inverse relationship between the org. culture about Compliance and ISP and the perception of Compliance as simply an administrative tasks.
- H4: There is a positive relationship between the perception of managers' behaviour regarding Compliance and the behavioural isomorphism (convergence) of other employees.
- H5: There is a positive relationship between the organisational role about ISP and compliant behaviour.
- H6: Organisational behaviour of managers and executives are perceived as a driving force influencing others to comply with ISP.

H7: Responses from managers and executives are different from those of the employees.

Relation between Hypothesis and Constructs		
Hypotheses	**Pertain to**	**Construct**
H1 and 2	→	WorkPlaceCulture
H3 and 4	→	Attitude
H5, 6 and 7	→	Actors

In order to verify the mentioned hypothesis within the framework of identified constructs, we included a number of control variables related to the characteristics of the answers. In order to account for the impacts of these characteristics on an employee's intention to comply with the ISP, an initial distinction was made between employees' and managers' responses. The variables were the baseline for the construction of the questionnaire.

The basic assumption for the structure of the variables was that the level of perception of an employee as well as his/her organisational position may influence compliant behaviour. This assumption is consistent with widely accepted and established literature (Ajzen and Fishbein, 1980; Ajzen, 1991; Dinev and Hu, 2007; Fishbein and Ajzen, 1975; Herath and Rao, 2009; Siponen et. al., 2010).

The composite grid of variables are summarized in the Table 2.

THE INSTRUMENTS

The proposed research model was tested through the survey method and the data collected. The sample consisted of 213 office employees, managers and executives, who responded via a questionnaire available on web, and the unit of analysis was the individual perception regarding the items of the questionnaire, derived from variables. As Compliance is always a thorny issue and

Table 2 Variables	
Variable	**Description**
V1	the perception of external motivation to abide by rules
V2	the perception of security threats as an influence on behaviour towards Compliance
V3	the personal favour about the importance of Compliance at any organisational level
V4	the knowledge and the perception about the consequences of non-compliant behaviour
V5	the reflection that a reward system for compliant behaviour is appropriate
V6	the personal convincing the IT plays a role in facilitating Compliance
V7	the perception that Compliance is an administrative task
V8	the perception about the influence of managers' behaviour
V9	the idea that the security-oriented tasks have a positive influence on Compliance
V10	the perception about the influence of the interaction with other employees which adopt a Compliance motivated behaviour
V11	the level of awareness of the Information Security Plan (ISP)
V12	the level of perception of the comprehension of the ISP
V13	the personal favour about the facilitating conditions that encourage compliant behaviour
V14	the perception about the statement that managers follow Compliance better then others
V15	the idea that Directors and Executives should enforce Compliance

Table 3 Demographics		
Occupation	**Count**	**%**
Board of Directors/Steering Committee/CEO (1)	80	37.96
CIO/IT Manager/CISO (2)	41	18.98
Business Manager (4)	7	3.24
IT Employee	5	2.31
Employee (Other than IT) (5)	77	36.11
Other (6)	3	1.39
No Answer	0	0.00
Total	213	100.00

any failure to observe legal requirements might entail prosecution, the anonymity of participants in the survey was assured by the lack of any form registration or IP logging.

Of the total of 216 questionnaires compiled, 213 were useable. Incomplete questionnaires were avoided making all questions compulsory in order to finish the questionnaire. The companies and individuals participating in the research were mainly Italian, with a small number of other EU based organisations.

Table 3 summarizes the demographic profile of the participants.

As mentioned above, the instrument was operational and based on previous studies into the beliefs, perceptions and compliant behaviour surrounding the socio-technical view of organisational issues.

The same measurement items used in those studies were applied to or adapted for this research.

The 5 measures of Workplace Culture were derived from Boss (2007), D'Arcy (2009) and Fishbein (2007), i.e. variables V1 → V5.

Personal Attitude was measured mainly from the point of view of Ajzen's Theory of Planned Behavior (Ajzen, 1991), i.e. variables V6 → V10.

The 5 measurements about Actors are from both Im and Baskerville's categories (2005), and from Siponen and Vance (2010).

For all measurement items, the 7 point Likert scale was used, with anchors ranging from strongly agree (1) to strongly disagree (7).

ANALYSIS AND RESULTS

All analysis was conducted utilising SPSS software. The 2 tail correlation significance test showed values of 95%, so correlation significance was verified. The internal reliability of significant variables was verified by performing a Crombach's α test, which showed values higher than 0.82. It should be noted that the alpha values might have been influenced by a slight redundancy between the items of the questionnaire, an intentional feature as a number of the variables were control variables. Correlation between significant variables was performed with the correlation index ρ.

ANOVA

The analysis of variance was computed on all data sets in order to obtain more accurate empirical evidence of the possible differences between panels. The ANOVA F test gave results regarding the 5 variables that suggested differences. A detailed analysis is given in the appendix.

DISCUSSION AND CONCLUSION

For the purpose of this research, we aimed at investigating the perception and the beliefs surrounding organisational issues such as Workplace Culture, Personal Attitude and those Actors deemed to be responsible for enforcing Compliance with the organization's ISP. In order to do this and search for evidence of a difference in their relative perception and beliefs, as derived from existent literature, two panels based on employee-type, average employees and managers/executives, were established. As hypothesized, it was found that Workplace Culture has a positive impact on the development of personal Attitude. This suggests that attitude has an antecedent in organisational culture. In line with this finding, evidence to confirm the validity of the hypothesis about the positive effect of external motivation (i.e. punishment) was collected. This finding suggests that the overall validity of external motivation is perceived as important, both by managers and employees. It is also interesting to note that the variable of IS threats as the antecedent for Compliance (V2) turned out to be a valid confirmation. This is primarily because we assume that a specific perception of threat may have differen-

Table 4
Basic statistics and Correlation about all sample

ALL SAMPLE	WPC					ATT					ACT				
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15
Mean	3,29	3,31	3,81	3,74	3,81	3,77	3,22	3,3	3,63	3,24	3,29	3,77	3,82	3,31	3,23
Median	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Mode	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
STD	0,83	0,88	1,29	1,28	1,08	1,06	1	1,09	1,04	1,07	0,87	1,31	1,3	1,11	0,81

Table 5
Basic statistics and Correlation on managers and executives panel

MANAGER and EXECUTIVES	WPC					ATT					ACT				
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15
Mean	3,32	3,23	3,67	3,55	3,57	3,67	3,3	3,45	3,56	3,32	3,39	3,63	3,62	3,42	3,32
Median	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Mode	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
STD	0,72	0,7	1,05	1,08	0,91	0,98	0,86	0,95	0,92	0,87	0,83	1,07	1,05	0,92	0,76

Table 6
Basic statistics and Correlation on employees panel

EMPLOYEES	WPC					ATT					ACT				
	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15
Mean	3,24	3,38	4,08	4	4,14	3,9	3,1	3,09	3,73	3,13	3,18	3,98	4,08	3,14	3,12
Median	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3
Mode	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3
STD	0,98	1,09	1,53	1,5	1,21	1,18	1,16	1,22	1,17	1,3	0,91	1,56	1,54	1,32	0,87

tial effects on Compliance. Research findings indicate that the inverse relationship between the belief that Compliance is just an administrative task and organisational culture is valid. This is rather encouraging as Compliance is often seen as mainly serving audit purposes rather than for reasons of security. Perception of this varies very little between the two panels. Hypotheses 1, 2 and 3 were completely supported by the evidence. As hypothesised, there is a strong common perception that the compliant behaviour of managers influences that of the other employees. This emerged as a belief shared by both panels. This result is consistent with literature (Burcu et al., 2010; Siponen and Vance, 2010) and thus Hypothesis 4 is upheld. With regard to the relationship between organisational role and compliant behaviour, the evidence showed that a member involved in the organization's environment focusing on information security, demonstrates

Table 7
Results of Hypothesis Test

	Hypothesis	Instr.	Support
1	Rewards for compliance with the ISP are positively perceived as beneficial	V1-V5	YES
2	Positive relation between organisational culture and personal attitudes	V3-V6/V9	YES
3	Inverse relationship between the org. culture about Compliance and ISP and the perception of Compliance as simply an administrative tasks	V7-V3	YES
4	Positive relationship between the perception of managers' behaviour about Compliance and the behavioural isomorphism of other employees	V10-V14	YES
5	Relationship between the organisational position about ISP and the compliant behaviour	V9-V12	YES
6	Organisational behaviour of managers and executives are perceived as a driving force influencing others to comply with ISP	V8-V15	YES
7	Responses for a managers and executives panel are different from those of the employees' panel	Median, mode ANOVA	NO PARTIAL

positive behaviour towards compliance. Whether this is a mere perception or a justified belief, it is a direct confirmation of hypothesis 5. All employees, managers and executives were positively oriented towards perceiving the driving force towards Compliance to be the duty of Senior Executives, Directors and Managers. This view was shared by both panels. The consequences of this common perception are that compliant behaviour is again related primarily to external drives and only in second place to internal drives, i.e. attitudes. Hypothesis 6 was thus confirmed. The conceptual consequences may suggest that, as organisational culture has proven to be an antecedent for personal attitude, the behaviour of Senior Management and Executives can be identified as the workplace culture. This by-finding offers scope for further investigation, which cannot be carried out using the present data set and instruments. Hypothesis number 7 was only partially confirmed by the results. It turned out that the median and mode of responses were equal. The measured mean and standard deviation do not yield grounds to contradict the evidence of the median and mode (tables 5 and 6). The ANOVA analysis, on the other hand, shows that for certain variables, 5 in total (V3, V4, V5, V8, V13), there was a significant difference between the two groups (panels). This was confirmed by the significance value of the F test <0,05 (i.e. 95%). There was no difference in responses about managers perceiving the adoption of better complaint behaviours compared with employees. All panels appear to agree on that belief.

LIMITATIONS

Any limitations in this research might be attributable to the type of instruments utilised to measure the perception and beliefs of the panel participants. There was no investigation into the actual levels of implementation of Compliance nor into effective compliant behaviour. This kind of measurement was not possible with the questionnaire method. A third of participants (approx. 37%) were CEOs, Directors and Executives and the perception of Compliance by top-level

management is based mainly on reports and official documents prepared for the Board of Directors which, by Italian law, is solely responsible for Compliance. Whilst these reports can be assumed to be reliable and truthful, at the very best they might not emphasize further action needed and really only highlight what has been already achieved with regard to Compliance. It is possible that the perception of Compliance and ISP held by these managers has been influenced by statements made in official documents. Although previous research has proven that a positive perception of ISP leads to better compliance behaviour (West, 2008; Warketin and Willson, 2009), this leaves an interesting starting point for more in-depth investigation. Another limitation can be found in the instruments utilised. The correlation between the variables was measured and not their "cause". Even though the research methodology was based on solid theoretical models, a number of different constructs or variables could be used in the future. It might be appropriate to repeat the investigation with the same individuals at a later date to test the consistency of the model and any change in perception and beliefs. Whilst participants responded to the questionnaire according to their own perceptions and beliefs, their answers may reflect their intentions rather than the facts. When expressing belief in the effect of some sort of punishment for non-compliant behaviour, they might be thinking in abstract terms rather than in reference to their own circumstances. Very rarely will an Executive receive punishment for non-compliant behaviour alone (if no harm or loss to company arises). The individual perception might change over time if, for instance, s/he receives punishment for non-Compliant behaviour. No distinction was made for the type of industry in which the participant worked nor for his/her age or gender. Further investigation into the relationship between these variables and those of this research would be of value. Finally, as some recent findings show that attitude plays a significant role in explaining the relationship between beliefs and intention (Burcu et al., 2010), it would be interesting to incorporate that assumption within the model of this research in order to develop these findings.

REFERENCES

Åhlfeldt R.M., Spagnoletti P. and Sindre G., 2007, Improving the Information Security Model by using TFI". In "New Approaches for Security, Privacy and Trust in Complex Environments", IFIP Springer Series, Springer Boston, Volume 232/2007, pag. 73-84, ISBN: 978-0-387-72366-2

Ajzen, I. and Fishbein, M., 1980, Understanding Attitudes and Predicting Social Behavior, Englewood Cliffs, NJ: Prentice- Hall.

Ajzen, I., 1991, Theory of Planned Behavior, Organizational Behavior and Human Decision Processes (50:2), pp. 179-211.

Ajzen, I. and Albarracin, D., 2007, Chapter 1: Predicting and Changing Behavior: A Reasoned Action Approach, in Prediction and Change of Health Behavior: Applying the Reasoned Action Approach.

Anderson, R. J., 2008, Security, Functionality and Scale?, in Vijay Atluri (Ed.): Data and Applications Security XXII, 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, London, UK, July 13-16, 2008, Proceedings. Lecture Notes in Computer Science 5094, Springer.

Anderson, R. J., 2009, Technical perspective - A chilly sense of security. Communication of ACM 52(5): 90 (2009).

Bodungen, C, Whitney, J and Paul, C. 2008, SCADA Security Compliance and Liability - A Survival Guide.

Boss, S. R. and Kirsch, L. J., 2007, The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines, in Proceedings of the 28th International Conference on Information Systems, Montreal, Dec. 9-12.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. European Journal of Information Systems (18:2), pp. 151-164.

Braccini A. M. and Spagnoletti P., 2008, Business Models and e-services: an ontological approach in a cross-border environment, in

D'Atri, A., De Marco, M., Casalino, N. Eds., Interdisciplinary Aspects of Information Systems Studies, Springer, Germany

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly, (34: 3) pp.523-548.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2004, Economics of IT Security Management: Four Improvements to Current Security Practices, Communications of the Association for Information Systems (14), pp. 65-75.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004a. A Model for Evaluating IT Security Investments, Communications of the ACM (47:7), pp. 87-92.

D'Arcy, J., Hovav, A. and Galletta, D., 2009, User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research (20:1), pp. 79-98.

Dhillon, G. 1997. Managing Information System Security, London: Macmillan.

Dhillon, G. and Backhouse, J. 2001. Current Directions in Information Security Research: Toward Socio-Organizational Perspectives, Information Systems Journal (11:2), pp. 127-153.

Dhillon, G. and Torkzadeh, G., 2001, Value-Focused Assessment of Information System Security in Organizations, in Storey, V., Sarkar, S., DeGross, J. I., (Eds.): Proceedings of the International Conference on Information Systems, ICIS 2001, December 16-19, 2001, New Orleans, Louisiana, USA. Association for Information System ICIS 2001:561-566.

Dhillon, G., Siponen, M. T., Sharman, R., 2005, Information Systems Security Management, 38th Hawaii International Conference on System Sciences (HICSS-38 2005), Proceedings, 3-6 January 2005, Big Island, HI, USA. IEEE Computer Society

Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," Journal of the Association for Information Systems (8:7), pp. 386-408.

Doherty, N. F., and Fulford, H. 2006. Aligning the Information Security Policy with the Strategic Information Systems Plan, Computers and Security (25:1), pp. 55-63.

Elffers, H., Heijden, P., and Hezemans, M. 2003. Explaining Regulatory Noncompliance: A Survey Study of Rule Transgression for Two Dutch Instrumental Laws, Applying the Randomized Response Method, Journal of Quantitative Criminology (19, 4), pp. 409-439.

Fishbein, M., and Ajzen, I. 1975. Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Reading, MA: Addison-Wesley.

Fishbein, M., 2007, A Reasoned Action Approach: Some Issues, Questions, and Clarifications, in Prediction and Change of Health Behavior: Applying the Reasoned Action Approach, in I. Ajzen, D. Albarracin, and R, Hornik (eds.), Hillsdale, NJ: Lawrence Erlbaum & Associates, pp. 281-296.

Freeman, E. H., 2007, Regulatory Compliance and the Chief Compliance Officer, Information Systems Security, 16:357–361, 2007

GAO, 2008, United States Government Accountability Office, GAO 08-280, Report to the Chairman of Securities and Exchange Commission, Information Security, Securities and Exchange Commission Needs to Continue to Improve Its Program, February 2008, [online] <http://www.gao.gov/new.items/d08280.pdf> [15 October 2010].

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R., 2006. CSI/FBI Computer Crime and Security Survey, Computer Security Institute <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf> [23 October 2010].

Herath, T. and Rao, H. R., 2009, Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations, European Journal of Information Systems (18), pp. 106-125.

Hu, Q., Hart, P., Cooke, D., 2007, The role of external and internal influences on information systems security – a neo-institutional perspective, Journal of Strategic Information Systems 16 (2007) 153–172.

Im, G. and Baskerville, R., 2005, A Longitudinal Study of Information Systems Threat Categories: The Enduring Problem of Human Error, The DATA BASE for Advances in Information Systems 36 (4) 68-79.

Lee, J.and Lee, Y., 2002, A Holistic Model of Computer Abuse Within Organizations, Information Management and Computer Security (10:2/3), pp. 57-63.

Mathieson, K., Peacock, E. and Chin, W., 2001, Extending the Technology Acceptance Model: The Influence of Perceived User Resources, The Database for Advances in Information Systems (32:3), pp. 86-112.

Melville, N., Kraemer, K. and Gurbaxani, V., 2004, Review: information technology and organizational performance: an integrative model of IT business value, MIS Quarterly 28 (2), 2004, pp. 283–322.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study, European Journal of Information Systems (18), pp. 126-139.

Neumann, P. G. 1999, Risks of Insiders, Communications of the ACM (42:12), pp. 160.

Pahnila, S., Siponen, M. and Mahmood, A. 2007, Employees' Behavior towards IS Security Policy Compliance, in Proceedings of the 40th Hawaii International Conference on System Sciences, Los Alamitos, CA, IEEE Computer Society, pp. 156-166.

Papadaki, M., Steven Furnell, S., Vulnerability management: an attitude of mind?, Network Security, Volume 2010, Issue 10, October 2010, Pages 4-8.

Ponemon, L. 2009, Trends in Insider Compliance with Data Security Policies, Ponemon Institute, USA.

Ponemon, L. 2009a, Cyber Security Mega Trends, Ponemon Institute, USA.

Schlarman, S., 2007. The IT Compliance Equation: Understanding the Elements, Information Systems Security, 16, pp. 224–232.

Siponen, M. T. 2005. An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. European Journal of Information Systems (14:3), pp. 303-315.

Siponen, M. T. and Vance, A. 2010, Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations, MIS Quarterly (34:3), pp. 487-502.

Siponen, M.T., Mahmood, M. A., Pahnila, S., 2009, Technical opinion - Are employees putting your company at risk by not following information security policies? Commun. ACM 52(12): 145-147.

Siponen, M. T., Pahnila, S. and Mahmood, A., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H. Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 133–144.

Siponen, M. T., Pahnila, S. and Mahmood, A., 2010, Compliance with Information Security Policies: An Empirical Investigation. IEEE Computer 43(2): 64-71.

Spagnoletti P. and Resca A., 2008, The duality of Information Security Management: fighting against predictable and unpredictable threats, Journal of Information Systems Security, Vol. 4 – Issue 3, 2008, ISSN Print 1551-0123 Online 1551-0808.

Spagnoletti P., Albano V., Caccetta E., Tarquini R., D'Atri A., 2011, Supporting policy definition in the e-health domain: a QCA based method, HEALTHINF – International Conference on Health Informatics, 26-29 January, Roma, Italy.

Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. 2005, Analysis of End User Security Behaviors, Computers and Security (24:2), pp. 124-133.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," Information Systems Research (1:3), pp. 255-276.

Straub, D. W. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly (22:4), pp. 441-469.

Techtarget 2010, [online] <http://searchdatamanagement.techtarget.com/definition/compliance>, [21 August 2010].

Thomson, M. E., and von Solms, R. 1998. "Information Security Awareness: Educating Your Users Effectively," Information Management and Computer Security (6:4), pp. 167-173.

Vardi, Y., and Weitz, E. 2004. Misbehavior in Organizations: Theory, Research, and Management, Hillsdale, NJ: Lawrence Erlbaum Associates.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," European Journal of Information Systems (18:2), pp. 101-105.

West, R., 2008, The Psychology of Security, Communications of the ACM (51:4), pp. 34-40.

Whitman, M. E. 2008. "Chapter 6: Security Policy: From Design to Maintenance," in Information Security: Policy, Processes, and Practices, D. W. Straub, S. Goodman, and R. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 123-151.

Whitman, M. E., Townsend, A. M., and Aalberts, R. J. 2001, Information Systems Security and the Need for Policy. Information Security Management – Global Challenges in the Next Millennium, G. Dhillon, London: Idea Group, pp. 9-18.