Communications of the IIMA

Volume 16 | Issue 4 Article 1

2018

End-users Compliance to the Information Security Policy: A Comparison of Motivational Factors

Peter Straver
HU University of Applied Sciences, peter@straver-ict.nl

Pascal Ravesteyn
HU University of Applied Science, pascal.ravesteijn@hu.nl

End-users Compliance to the Information Security Policy (ISP): A Comparison of Motivational Factors

INTRODUCTION

Business information plays an important role for most organizations (Ifinedo, 2014; Moody, Siponen, and Pahnila, 2018). To compete in today's business environment, organizations rely heavily on information systems. The protection of the business information held in such information systems has emerged as a key managerial priority (Ifinedo, 2014; NEN-ISO-27002, 2013). Organizations need security controls to proactively protect their valuable information, considering today's threatened cyber environments (Knapp, Morris, Marshall, and Anthony, 2009; Moody et al., 2018).

It is well known among cyber security practitioners, that many human factors affect information security management (Acuña, 2016). In a study on the cost of data breaches at 314 organizations by Ponemon Institute (2014) it is found that 30% of the root causes for data breaches are related to employees or contractors. Employees not adhering to information security policies is a serious threat to an organization (Siponen, Mahmood, and Pahnila, 2009; Willison, Warkentin, and Johnston, 2018). Hindrance caused by security practices is one of the reasons employees dislike such practices (Herath and Rao, 2009a).

It is recognized that one approach for making information security effective within organizations is to promote correct (in line with security policies) end-user behaviors and constrain bad end-user behaviors (Karwowski and Glaspie, 2018). To give direction to these behaviors a solution is found in information security policies which define the concepts and processes of information security (Knapp et al., 2009; Mears and Von Solms, 2007; Sohrabi Safa, Solms, and Furnell, 2015). Organizations need to focus on their non-malicious employees' intentions and behaviors towards compliance to the organizations information security policy (Ifinedo, 2014).

Therefore, within a context of information security, organizations can focus on conditions likely to promote motivational factors influencing the individual's intentions to perform desired behavior (Ajzen, 1991; Ifinedo, 2014; Ryan and Deci, 2000; Stanton, Stam, Mastrangelo, and Jolton, 2005; Weber, Otto, and Osterle, 2009). In the end, the individual's intentions should lead to the desired behavior of compliance to the Information Security Policy (ISP) which in turn leads to an increased level of protection of the organization's information and technology resources (Sohrabi Safa et al., 2015).

Several motivational factors influence the intentions of end-users to comply with their organizations ISP. However, it is unclear which factors are the most relevant. Therefore, in this paper we research the following question: *What motivational factors relate, in which degree, to intentions on compliance to ISP and how could these insights be utilized to promote end-users compliance within a given organization?*

The goal of this research is to provide more insight in the motivational factors applicable to ISP and their influence on end-user behavior, thereby broadening knowledge regarding information systems security behaviors in organizations from the viewpoint of non-malicious abuse and offer a theoretical explanation and empirical support. The outcomes are also useful for practitioners to complement their security training and awareness programs, in the end helping enterprises better effectuate their information security policies.

In this study an instrument is developed that can be used in practice to measure an organizational context on the effects of six motivational factors recognized. These applicable motivational factors are determined from literature and subsequently evaluated and refined by subject matter experts. A survey is developed, tested in a pilot, refined and conducted within four organizations. From the statistical analysis, findings are reported and conclusions on the hypothesis are drawn.

The remainder of this article is structured as follows. In Section 2 an overview of the theoretical background is presented. In Section 3, a framework is constructed leading to a final conceptual model and hypotheses. In Section 4 the framework is operationalized by developing a survey instrument to collect data. In Section 5 the instrument is applied within organizational contexts. The article concludes with section 6 where conclusions are provided and implications are discussed.

RELATED LITERATURE

Information Security often gives an additional workload which creates a conflict of interest between functionality and information security (Albrechtsen, 2007). To help information security managers diagnose the deficiencies in their Information Security Management approach and solve behavioral issues, an understanding of what factors motivate employees to comply to ISP is needed (Bulgurcu, Cavusoglu, and Benbasat, 2010).

From the analysis of literature, research areas with a focus on influencing malicious and/or non-malicious behavior are determined. Literature was found using (combinations of) keywords such as information security policy, governance, risk management, motivation, awareness, behavior, intentions, compliance, privacy, countermeasures, data management, ethics, ownership, violation, job performance and neutralization. The process of tracing back on references within the found literature brought additional insights on influencing malicious and/or non-malicious behavior of employees regarding ISP within organizations. Different research areas with a focus on influencing malicious and/or non-malicious behavior have been researched in the past years (Sohrabi Safa et al., 2015). Table 1 shows an overview of the literature found in different research areas and related focus, which are described in the remainder of this section.

Table 1: Overview of literature.

Research area	Focus	Author; specific aspect (if applicable)
Deterrence	Malicious	(Straub, 1990); As control against abuse. (Straub and Welke, 1998); As risk countermeasure. (D'Arcy, Hovav, and Galletta, 2009); On user awareness.
Fear	Malicious	(Johnston and Warkentin, 2010) (Johnston, Warkentin, and Siponen, 2015); On sanctioning aspect.
Neutralization	Malicious + Non-malicious	(Siponen and Vance, 2010) (Willison and Warkentin, 2013)
Ownership	Malicious + Non-malicious	(Spears and Barki, 2010) (Mosley, 2008) (based on DAMA DMBOK) (Pierce, Kostova, and Dirks, 2001, 2003)
Rationality and Awareness	Non-malicious	(Bulgurcu et al., 2010)
Planned Behavior and Protection Motivation	Non-malicious	(Ifinedo, 2012)
Information Security Governance	Non-malicious	(Andersen, 2001) (Posthumus and Von Solms, 2004) (Von Solms, 2006) (Veiga and Eloff, 2007)

Area of Deterrence theory: One way to influence end-user behavior is using deterrence approaches as countermeasures to computer abuse like described by Straub (1990). One implication of that study is the positive effect of an active security staff and a commitment to involving end-users in data security. The involvement of the end-users is relevant within this research as another conclusion of Straub is that articulation (in the sense of formalization) of the policy and actively enforcing the policy leads to a benefit in information security. In the light of deterrence, the knowledge and perceptions of users on the consequences of abuse are of major importance.

Straub and Welke (1998) mention deterrence as one of the countermeasures in their 'Countermeasure Matrix' which consists of four countermeasures: deterrence, prevention, detection and remedies. The 'Countermeasures Matrix' used in conjunction with the 'Security Risk Planning Model' Straub and Welke developed, forms an approach to efficiently and effectively formalize parts of the security system.

This is supported by D'Arcy et al. (2009) who found that user awareness of security policies combined with monitoring (similar to 'prevention' and 'detection' of the before mentioned 'countermeasures matrix' (Straub and Welke, 1998)) have a deterrent effect on the intention to misuse information systems. Sanctions should be part of any deterrence strategy and especially the perceived certainty and/or severity of these sanctions play a role towards the end-users.

Area of Fear: An investigation on the influence of 'fear appeals' on the compliance of end-users has been conducted by Johnston and Warkentin (2010). A 'fear appeal' is a persuasive message that attempts to arouse fear in order to divert behavior through the threat of impending danger or harm (Maddux and Rogers, 1983). The purpose of the investigation was to examine the influence of fear appeals on behavioral intentions, specifically the compliance of end-users to ISP. Johnston and Warkentin discovered an impact on the end-users behavioral intentions to comply to ISP when certain fear-inducing arguments come into play. Their findings are not consistent across all end-users, the individual impact is based on the individual end-users perceptions of efficacy and threat (Johnston and Warkentin, 2010).

Recently Johnston, Warkentin and Siponen (2015) continued their research in fear and sanctioning, extending the concept of fear appeals as a common tool to motivate individuals in their policy compliance intention. However, because of the mixed results of the 2010 study the dimension of personal relevance is added to the original model in order to enhance its effectiveness. The efficacy of the 'enhanced fear appeal' framework is validated empirically providing a significant positive influence on compliance intentions.

Area of Neutralization: Neutralization, which includes different factors like 'defense of necessity' and 'denial of responsibility', is another research domain related to policy compliance intention. Neutralization is a prominent theory in the field of Criminology and is applied by Siponen and Vance (2010) in the context of information systems. Siponen and Vance propose a theoretical framework to measure the effects of neutralization techniques alongside those of the sanctions described by deterrence theory. When developing and implementing organizational security policies and practices, neutralization should be a factor to take into account. Again, compliance intentions is the center of the proposed framework (Siponen and Vance, 2010).

Purely focusing on deliberate and malicious insider computer abuse, Willison and Warkentin (2013) extended the Straub and Welke (1998) security action cycle framework. They propose techniques of neutralization (rationalization), expressive/instrumental criminal motivations and disgruntlement as a result of perceptions of organizational injustice as three areas worthy of further empirical investigation. Thereby bringing to attention that "emotions may impact deterrence efficacy with regard to employee computer abuse. However, could this not also be the case with regard to policy compliance by employees?" (Willison and Warkentin, 2013). This question on the impact of emotions is taken into account in the intrinsic motivation part of the conceptual model for this research.

Area of Ownership: Demonstrated Ownership as a means to increase end-users participation in protecting sensitive information was investigated as factor to compliance. The data was collected via a survey of 228 members of ISACA (Mosley, 2008), the association behind DAMA DMBOK framework. This framework lists the users to be a resource to information systems security (Spears and Barki, 2010). The study by Spears and Barki is a primary source of the 'Data Ownership' factor in the conceptual model for this research and also includes knowledge from other frameworks like ISO 17799:2000 (since 2007 aligned with ISO 27000-series (NEN-ISO-27001, 2013; NEN-ISO-27002, 2013)).

Sense of ownership refers to the state where people develop feelings of ownership for a variety of objects, material and immaterial in nature (Pierce et al., 2003). For example a company car, or in the focus of this research an organization's information asset covered by the organization's ISP. A conclusion by Pierce, Kostova and Dirks (2001) is that psychological ownership has emotional, attitudinal and behavioral effects on those that experience ownership. Besides psychological ownership, an employee's 'organizational commitment', which is defined as the overall strength of an individual's identification with, and involvement in, an organization is also likely to play a role in his/her engagement in security (Herath and Rao, 2009a).

Area of Rationality and Awareness: Bulgurcu et al. (2010), similarly to our study, focus on non-malicious abuse and the recognition that employees, being the end-users of information systems, can be great assets in the effort to reduce risk related to information security. More specific Bulgurcu et al. study rationality based factors behind an end-users drive to comply to

policy. Attitude is placed in the center of the model as a main contributor to the intention to comply to policy. Attitude in the 'model of antecedents' is influenced by benefit and cost of compliance and the cost of non-compliance. Attitude is also influenced by information security awareness. Especially the hypothesis: "An employee's attitude toward compliance with the organization's ISP positively affects intention to comply with the requirements of the ISP" (Bulgurcu et al., 2010) is of interest to our study. Bulgurcu et al. conclude that 'attitude' is an important mediator in explaining the relationships between information security awareness and the intention to comply.

Area of Planned behaviour & Protection motivation: Ifinedo (2012) combines the theory of planned behavior (TPB) and the protection motivation theory (PMT) to show that the factors within those theories have an influence on intention to comply. Again, attitude is found to be the most significant factor to influence intention, thereby supporting Bulgurcu et al. Guo, Tyan, Archer and Connely (2011) also studied attitude with a strong focus on end-user intentional and non-malicious actions. They found that linking security and business objectives by cultivating a culture of secure behavior in organizations is important.

In contrast, end-users strive to meet their job performance expectations. It is demonstrated that end-users of information systems are goal oriented which might cause them to 'be required' to violate ISP. Such expectations strongly influence attitudes of end-users towards compliance (Guo et al., 2011).

Area of Information Security Governance: According to (Posthumus and Von Solms, 2004) "Information security governance is a complex issue requiring the commitment of everyone in an organization to do their bit in order to protect their company's valuable business information assets." Issues related to governance are also discussed by Hoogervorst (2009) in his study a distinction is made between Corporate Governance, IT Governance and Enterprise Governance. Information Security Governance, according to Von Solms (2006), is an integral part of Corporate Governance, and consists out of several elements working together to ensure that the confidentiality, integrity and availability of the company's assets (data, information, software, hardware, people etc.) are maintained at all times.

FRAMEWORK CONSTRUCTION

As described above the field of knowledge related to 'Policy Compliance' is studied to provide the theoretical foundation to this research. Based on this, two explorative sessions with subject matter experts were organized. From these sessions it was found that several factors surrounding compliance to ISP had also been researched in relation to policy compliance in practice. The combination of the findings of the literature study and the outcomes of the expert sessions resulted in a conceptual model consisting of 4 high-level factors that are expected to have a positive relation to Policy Compliance Intention (PCI).

Two such factors (**Social Pressures** (subdivided in 2 elements being Normative Beliefs and Peer Behavior) and **Effect of actions** (consisting of the single element Perceived Effectiveness)), as discussed and validated by Herath and Rao (2009b), are adopted in the conceptual model of this research as their model has shown to be of value to information security researchers (Bulgurcu et al., 2010; D'arcy and Herath, 2011; Siponen and Vance, 2010+2013). Their study made a contribution towards understanding the problem of encouraging employee information security behaviors using a theoretically well-grounded

approach based on micro-economic, sociology and psychology principles (Herath and Rao, 2009b).

Furthermore, the following two factors from literature that were found in relation to policy compliance are included in the model:

- **Information Security Governance (ISG)** (recognized in relation to compliance by several publications (Andersen, 2001; NEN-ISO-27002, 2013; Posthumus and Von Solms, 2004; Von Solms, 2006; Veiga and Eloff, 2007))
- **Sense of ownership** (recognized in relation to compliance by several publications (Mosley, 2008; NEN-ISO-27001, 2013; Pierce et al., 2001, 2003; Spears and Barki, 2010))

Although these factors are recognized in relation to compliance to ISP both Information Security Governance (ISG) and Sense of ownership are not yet researched as a motivational factor related to compliance to ISP. Because of this current lack of insight in regards to these factors on the intention of end-users to comply with ISP, determining system risks may be less effective. Researching these additional factors supports the goal of this research.

Factor 'Information Security Governance' is added to the model and subdivided into two motivational elements as recognized in literature to be extrinsic motivational elements for Information Security Governance:

1a) The first element is the existence of a formally expressed 'Data Custodian' role (a custodian is looking after the assets on a daily basis, but the responsibility remains with the owner (Cupoli, 2014; NEN-ISO-27002, 2013)) together with
1b) the existence of a formally expressed 'Data Steward' role (the careful and responsible management of something entrusted to one's care (Dawes, 2010; Educause, 2009))
2) The second element is the existence of formally expressed regulation on 'Information Classification' (an indicator on Confidentiality, Integrity and Availability based on criticality and sensitivity of the information (Johnston and Hale, 2009; Puhakainen and Siponen, 2010))

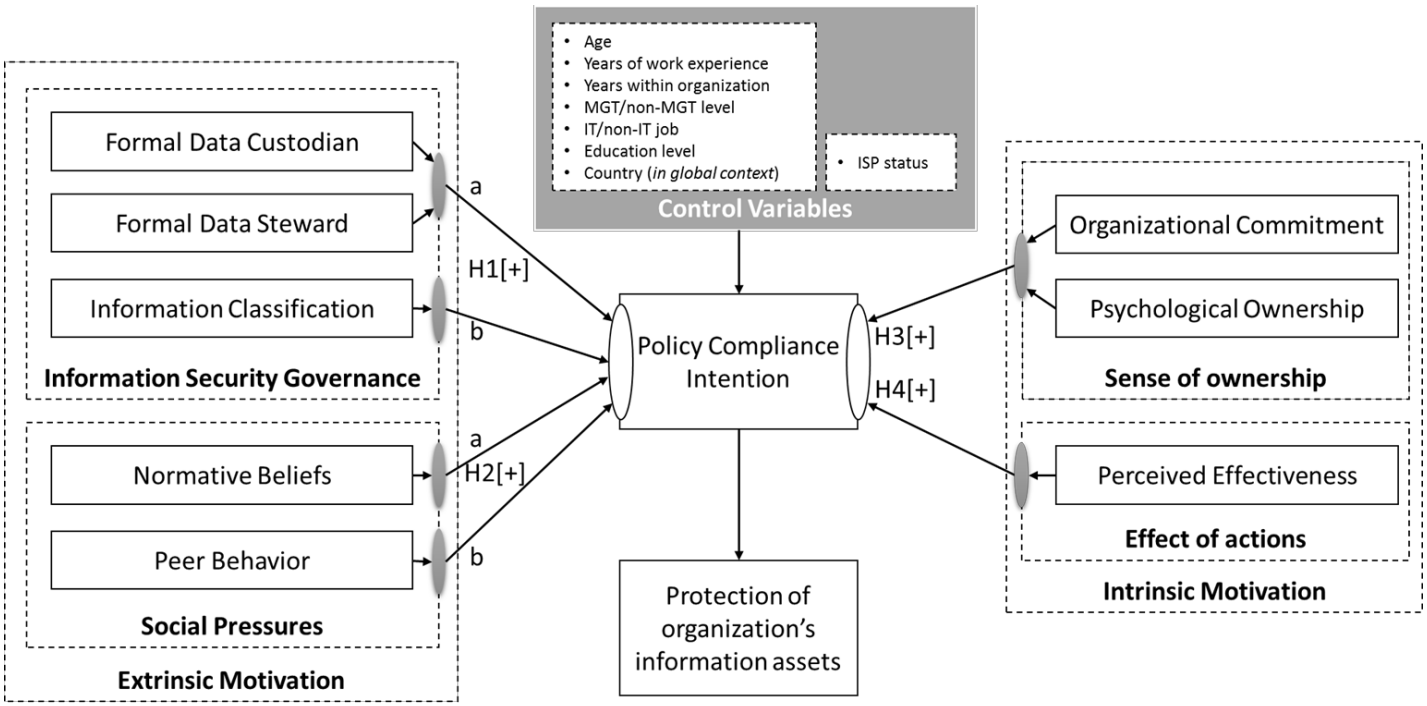
Factor 'Sense of Ownership' is added to the model as a single motivational element as recognized in literature to be intrinsic consisting of 2 parts:

1) The first part is 'Psychological Ownership' which is characterized by the personal motivation to protect the object of ownership, which can include an entity, idea or mission (Avey, Avolio, Crossley, and Luthans, 2009). Also, Spears and Barki (2010) found a strong relationship on ownership in their research on user participation in information systems risk management which strengthens the choice to position ownership as a motivational factor within the expanded model.
2) The second part is 'organizational commitment', which is defined as the overall strength of an individual's identification with, and involvement in an organization, which is also likely to play a role in his/her engagement in security (Herath and Rao, 2009a).

More on sense of ownership is found in the research by Van Dyne and Pierce (2004) on the importance of 'feelings of ownership' for the organization, even when employees are not the legal owners. Organizational commitment can be reflected in three components where each component is considered to have different implication for on-the-job behavior (Meyer and Allen, 1991). Research showed the linkage between organizational commitment and information security (Olckers, 2013; Stanton, Stam, Guzman, and Caledra, 2003).

The resulting conceptual model shown in Figure 1 contains one dependent variable (Policy Compliance Intention (PCI)), being influenced by four main motivational factors constructed from a total of six motivational elements found in the literature forming the independent variables. To control whether other variables have an influence on PCI, some control variables and demographics are in the model as well. The model shows the relationships to be researched within the specific context of a given organization.

Figure 1: Conceptual Model.



Based on the conceptual model the following hypotheses are formulated:

H1a Data Governance positively influences Policy Compliance Intention
H1b Information Classification positively influences Policy Compliance Intention
H2a Normative Beliefs positively influences Policy Compliance Intention
H2b Peer Behavior positively influences Policy Compliance Intention
H3 Sense of ownership positively influences Policy Compliance Intention
H4 Effect of actions positively influences Policy Compliance Intention

Some control variables are included in the model to test whether these demographics affect the dependent variable (Siponen and Vance, 2010). Based on earlier research (D'Arcy et al., 2009) it is expected that some of the control variables will have a significant effect on the variance of "Policy Compliance Intention".

In the next section, we describe how the framework is operationalized by developing a measurement instrument.

DATA COLLECTION

In order to operationalize the model, survey questions used in the research of Herath and Rao (2009b) are reused and additional questions on the added factors Information Security Governance and Sense of ownership are formulated to measure the perceptions of the end-users within an organizational context, on the motivational factors of the model. Also the analysis methods are pre-determined. To test the research instrument, a survey is conducted within a pilot context after which the results are analyzed in order to refine the research instrument where applicable.

The survey consists of at least two questions per relationship element in the conceptual model where each answer is given on a Likert (Likert, 1932) type scale that indicates a respondent's level of agreement with the statement regarding the likelihood of complying with the information security policies in their organization. Existing scales are used to measure the constructs in this research (Bulgurcu et al., 2010; Herath and Rao, 2009a; Siponen and Vance, 2010) which consists of 5 points rating from Strongly disagree, Disagree, Neutral, Agree to Strongly agree.

With the conceptual model as a starting point, all factors have a mapping to at least two sources of literature. The survey is developed in both a local language and an international edition. For the already validated part of the model based on Herath and Rao (2009b) the questions are reused as well as translated to Dutch and converted when needed. The term 'converted' implies minor textual/grammatical changes in order to align translation between the local language (Dutch) version and the international version (in English, as provided in Appendix A). For the elements in the factors Sense of ownership and Information Security Governance questions are formulated based on our literature study. To get insight into the context and status of the policy, several questions are included to determine the status and perception around ISP. All elements and variables are shown in Table 2.

Table 2: Survey questions and variables.

Element	Variable abbreviation	Nr. of questions
Policy Compliance Intention (dependent variable)	PCI	3
Effect of actions: Perceived Effectiveness (independent variable)	EFF	2
Social Pressures - element: Normative Beliefs (independent variable) - element: Peer Behavior (independent variable)	 NORM PEER	 5 3
Sense of ownership - element: Organizational Commitment and Psychological Ownership (independent variable)	COMMIT+OWN	2+3
Information Security Governance - element: Formal Data Custodian and Formal Data Steward (independent variable) - element: Information Classification (independent variable)	 CUSTO+STEW CLASS	 2+2 3
Information Security Policy status (context input)	ISP	6

Each element in Table 2 has an abbreviated variable used to code the questions for the statistical process in the 2nd column. To control for explanation of results due to other factors, several control variables were added as shown in Figure 1. These include demographic characteristics of the individual respondent. Age, years of work experience, years within organization, the job level in the organization and educational level were included to determine an individual's

position within an organization in order to determine the influence of these variables on the intentions. To control whether being part of ICT department is of any influence on intentions, the respondents are also asked whether they are within the ICT department. To get more feeling on the context and status of the policy, several questions are included measuring status and perception around ISP (Information Security Policy).

Especially in research studies where individuals are asked to report their 'intention to comply' there is the potential for response bias, social desirability bias and therefore political incorrectness (Siponen and Vance, 2013). This concern is minimized by informing the participants that the submission of truthful responses would never yield negative consequences.

In order to validate and refine the research instrument before widely deploying the instrument, a company in the business of ICT Security (context 1), located in the Netherlands with a focus on Dutch customers, participated in a pilot survey. For this company the areas of Information Security and ISP are very relevant, because all core activities of this company have to do with these expertise areas. The pilot instrument is send to a total of 100 employees from which 57 persons responded in full.

Subsequently these responses were analyzed to determine the applicability of our analysis methods as well as the measurement instrument. Based on this the measurement instrument (the survey) is revised to the final instrument presented in Appendix A. After this, four more organizations (context 2 till 5) send out the distribution email for participation in the final survey. Each organization (context) was given the same amount of time to fulfil the survey. A brief description per context is found below:

- **Context 2:** Healthcare Consultancy and Insurance company founded over 90 years ago. The Insurance unit is subject to supervision by the Dutch prudential supervisor 'De Nederlandsche Bank'. The current ISP dates from 2010, based on on-premise ICT services while in the meantime a great amount of outsourcing took place following their sourcing strategy of the past years. Current ISP is formalized by the management team and above. Physical information as well as electronic information is covered by the ISP.
- **Context 3:** Marketing Technology organization founded in 1992 that through numerous acquisitions together with research and development activities turned into a global player in their field of work. As a commercial organization in rapidly evolving market conditions, a strategic link to harness their competitive positioning makes ISP compliance very relevant. All end-users working at the 'DevOps' unit/part of the organization are selected to conduct the survey.
- **Context 4:** Retail organization founded in the 1820's currently operating over 5700 stores around the globe. Just after the start of the new millennium they took over a large retailer group and became dominant in BeNeLux area. With the increasing adaption and application of IT in their business, information has become a critical company asset and therefore information security has become an important responsibility for everyone in the organization. Dutch HQ employees are selected to conduct the survey.
- **Context 5:** Financial escrow services organization which operates as an independent third party service provider in the management of mortgages and consumer loans. Offering these services brings a great responsibility on information security. The full organization is part of the context. All end-users of information systems are requested to conduct the survey.

Table 3 shows the status after closing the surveys. From the 993 survey requests a sum of 371 valid responses is collected.

Table 3: Response rates on final surveys.

	Context 2	Context 3	Context 4	Context 5		Total
# of requests for filling out the survey	403	180	110	300	→	Sum of 993
Valid responses	123	81	51	116	→	**Sum of 371**
Response rate	30,52%	45,00%	46,36%	38,67%	→	**Average: 40,14%**

Statistical Package for the Social Sciences (SPSS) version 22 software is used to analyze the survey data. Measurement validation and structural model testing took place using the below steps:

1) **Import** measured variables into SPSS dataset for analysis and remove partial/incomplete responses.
2) **Recode** variables into positive measurements (in case of inverted questions) and recode textual variables into numerical values.
3) **Factor analysis** of all items to determine how well the items, that are supposed to represent one construct, separate from the items that are supposed to represent a different construct (Urdan, 2010).
4) **Reliability analysis** of the items belonging to each factor to determine how well the items in each of the elements (multi-faceted constructs) of the conceptual model, as a group (factor or element(s) of factor) go together. The Cronbach's alpha indicates how well the items within each of the factors measure the single underlying construct of each hypothesis. "This similarity of responses indicates that the construct is being measured reliably by all of the items." (Urdan, 2010, p. 178)
5) **Multiple regression analysis** testing the ordinal variables of the determined factors and elements by determining the relative strength of each predictor variable and determine the way each variable contributes as a predictor. (Urdan, 2010, chap. 13).

RESULTS

Based on the data that is collected analyses are conducted. Data is imported and recoded to the variables listed in Table 2 and textual variables are turned into numerical values forming the dataset to analyze.

A factor analyses is conducted on all items measuring the motivation factors and PCI. This factor analysis, using principal components extraction and varimax with Kaiser Normalization factor rotation, produced the expected 7 factors (the dependent and the 6 independent elements) with eigenvalues greater than 1.0. Suppressing absolute values below 0,326 gives the rotated result as shown in Table 4.

Table 4: Factor Analysis.

Rotated Component Matrix

	Component						
	1	2	3	4	5	6	7
EFF1						,915	
EFF2						,900	
NORM1	,794						
NORM2	,804						
NORM3	,756						
NORM4	,826						
NORM5	,832						
PEER1							,846
PEER2							,851
OWN1			,831				
COMMIT1			,833				
COMMIT2			,778				
CUSTO1		,722					
CUSTO2		,790					
STEW1		,749					
STEW2		,740					
CLASS1				,739			
CLASS2				,899			
CLASS3				,839			
INT1					,725		
INT2					,756		
INT3					,809		

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

The outcomes of the factor analysis in Table 4 provides evidence that the items in the survey belong together as per how the factors were constructed. Besides a factor analysis a **reliability analysis** is performed (see Table 5), as can be seen all factors are being measured reliably with scores above 0,7 by the underlying items (Urdan, 2010, p. 178).

Table 5: Reliability analysis for research contexts.

Factor / element	Measurement	Comment
Policy Compliance Intention **INT1 INT2 INT3**	$\alpha = 0{,}827$	**Reliable**
Normative Beliefs **NORM1 NORM2 NORM3 NORM4 NORM5**	$\alpha = 0{,}892$	**Reliable**
Effect of actions **EFF1 EFF2**	$\alpha = 0{,}878$	**Reliable**
Peer Behavior **PEER1 PEER2**	$\alpha = 0{,}743$	**Reliable**

Data Governance **CUSTO1 CUSTO2 STEW1 STEW2**	α = 0,782	**Reliable**
Information Classification **CLASS1 CLASS2 CLASS3**	α = 0,863	**Reliable**
Sense of Ownership **COMMIT1 COMMIT2 OWN1**	α = 0,842	**Reliable**

For the dataset a **multiple regression analysis** is conducted to examine the predictors of the dependent Policy Compliance Intention factor. Together, these predictors account for 41% (adjusted R2 = 0,409) of the variance in PCI (Policy Compliance Intention). Five of these variables were significant predictors of PCI. Adding the sixth variable Data Governance to the model doesn't raise the adjusted R2 of the model.

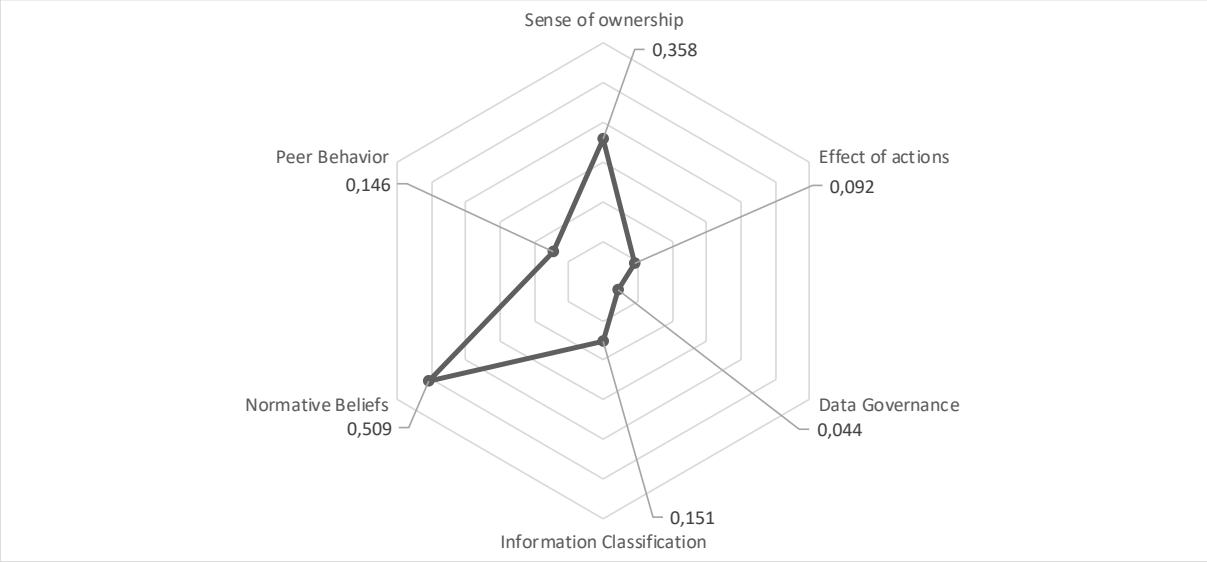
The measured coefficients during analysis show significant paths at the p = 0.01 level for four of the predictors:

- Normative Beliefs (element of factor Social Pressures)
- Sense of ownership
- Information Classification (element of factor Information Security Governance)
- Peer Behavior (element of factor Social Pressures)

Effect of actions shows significant paths at the $p = 0.05$ level. Data Governance (combination of Custodian and Steward and element of factor Information Security Governance) does not show significant paths in the model in the generalized dataset.

Analysis of the dataset shows an averaged image of the paths for all research contexts as shown in Figure 2.

Figure 2: Path coefficients research contexts per factor.



The coefficients values for Figure 2 are summarized in below Table 6.

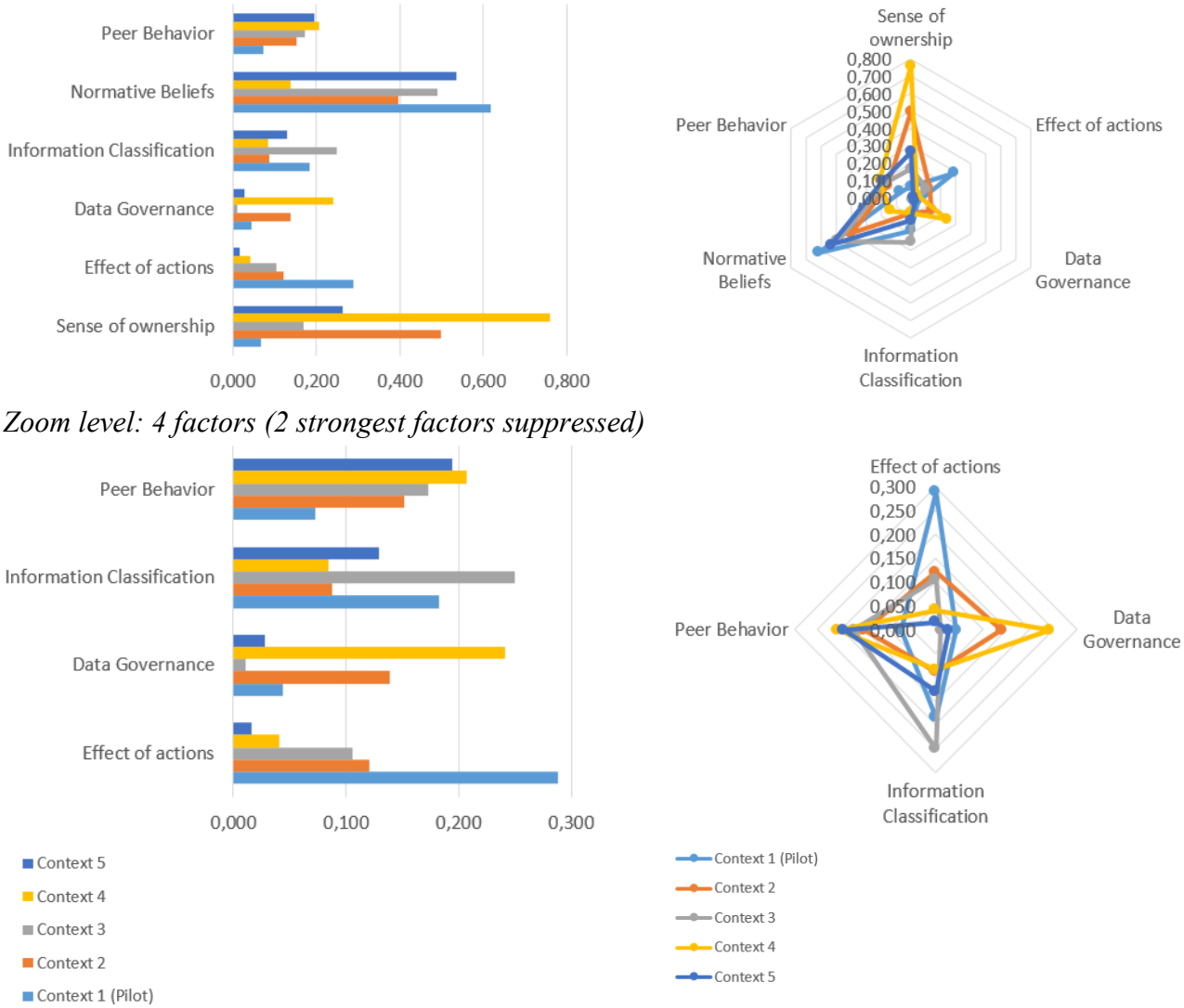
Table 6: Path coefficients for research contexts.

Dependent variable	Predictor	Beta	Adjusted R^2
Policy Compliance Intention	Sense of ownership	β = 0,358	40,91
	Effect of actions	β = 0,092	
	Data Governance	β = 0,044	
	Information Classification	β = 0,151	
	Normative Beliefs	β = 0,509	
	Peer Behavior	β = 0,146	

When applying different 'zoom levels' on the radars and plotting the paths in bar charts, thereby suppressing the 2 strongest factors, a better insight is given on the variance of the other 4 factors per context. The effect is seen in Figure 3 where also the pilot context is displayed for comparison of results.

Figure 3: Comparison of contexts.

Zoom level: 6 factors



Zoom level: 4 factors (2 strongest factors suppressed)

Based on this we conclude that: *a generalized view on the motivational factors could provide value however, the motivational factors should be measured per context to determine if an organization needs targeted advice on their organization specific security program.*

CONCLUSIONS AND FURTHER RESEARCH

As hypothesized, in general, positive influences on all recognized relationships are found in the research findings as shown in Table 7:

Table 7: Results on hypothesis

Nr.	Hypothesis	Result
H1a+	Data Governance positively influences PCI	Supported*
H1b+	Information Classification positively influences PCI	Supported
H2a+	Normative Beliefs positively influences PCI	Supported
H2b+	Peer Behavior positively influences PCI	Supported
H3+	Sense of ownership positively influences PCI	Supported
H4+	Effect of actions positively influences PCI	Supported*

* *Measurements show that these factors are missing any relevance for some of the contexts but do show significant relevance for another context.*

From the research findings the following conclusions are drawn:
First, "Normative beliefs" as an extrinsic motivational factor, has a strong relation to compliance to ISP. Shaping conditions influencing this specific factor can therefore be very effective for any organization or context.

As a suggestion, to utilize this insight in practice organizations can focus on the referents of the end-users such as executives, colleagues and managers. They should express their expectations about compliance with the requirements of the ISP to their referrers. This is in line with the findings of Bulgurcu et al. (2010), Herath and Rao (2009b) and Ifinedo (2014) whom stated that normative beliefs are based on the belief as to whether or not a significant person wants the end-user to perform the expected behavior.

Second, "Sense of ownership", as an intrinsic motivational factor, has a strong relation to compliance to ISP. Shaping conditions influencing this specific factor can therefore be effective for any organization or context.

As a suggestion, to utilize this insight in practice organizations can focus on conditions empowering and allowing end-users to exercise a certain level of control over important aspects of their work arrangements. According to earlier research conducted Avey, Avolio, Crossley, and Luthans (2009), Van Dyne and Pierce (2004), Mayhew, Ashkanasy, Bramble, and Gardner (2007) and Spears and Barki (2010) by aspects like job satisfaction and self-esteem improve sense of ownership. This means that implementing conditions around "normative beliefs" and "sense of ownership" always provides a positive influence to compliance, despite the context.

Finally, the other motivational factors should first be measured within the specific organization context to determine their relevance to that specific context. The relevance of each factor measured within a context determines the prioritization on shaping conditions influencing these specific factors. Using an approach focused on a specific context can therefore be very effective within that context.

Suggestions to utilize the insights from this research in practice are provided for each factor below:

- **Effect of actions**, as an intrinsic motivational factor, can be utilized in practice if the specific organization focusses on giving end-users the possibility of being in control and being able to effect a desirable outcome of actions. If employees believe that their actions can make a difference and have an impact on the overall organizational information security goal, they are more likely to undertake security behaviors (Avey et al., 2009; Herath and Rao, 2009b; Olckers, 2013).
- **Data governance**, as an extrinsic motivational factor, can be utilized in practice if the specific organization focusses on formalizing data governance aspects within the organizations ISG. This includes, besides other aspects, defining policies and procedures to ensure proactive and effective data management using roles such as data custodian and stewards at the tactical level of the organization. It is important for an organization to structure an organization-specific data governance model (Cheong and Chang, 2007; Lee and Strong, 2003; NEN-ISO-27002, 2013; Weber et al., 2009).
- **Information Classification**, as an extrinsic motivational factor, can be utilized in practice if the specific organization focusses on formalizing information classification aspects within the originations ISG. Besides formalizing information classification schemes organizations should also take care on the more practical aspects. For example, users should have the skills to apply the scheme. This means recognizing confidential information and applying the correct security measures. Another aspect found in this factor is the hinder of such measures, which should be as low as possible, to promote end-users to keep classifying on the right level, instead of a lower level for convenience or compatibility reasons (Johnston and Hale, 2009; Puhakainen and Siponen, 2010; Veiga and Eloff, 2007).
- **Peer behavior**, as an extrinsic motivational factor, can be utilized in practice if the specific organization focusses on putting desired behavior in the spotlight. Such social pressures exerted by norms and co-worker behaviors positively influence end-users intentions. Behavior follows behavior: "if everyone is doing it, it must be a sensible thing to do" (Cialdini, Reno, and Kallgren, 1990). End-users seeing their co-workers routinely follow ISP are likely to carry out similar behaviors (Cheng, Li, Li, Holm, and Zhai, 2013; Cialdini et al., 1990; Fishbein and Ajzen, 1975; Herath and Rao, 2009b, 2009a).

Limitations

As with all studies also this research has limitations. A key limitation of this research is the sample size per organization. Data was collected from organizations within different sectors but in each of these sectors only one organization participated. Therefore the findings cannot be generalized for a sector or be deemed reliable in general. Although our model seems to be consistent based on our data set more research is needed to test this. So, to further enhance the recommendations, more insights and knowledge on the motivational factors could be gained by applying the instrument to more organizations within the same sector in future research. Such research could provide further insights on the specific motivational factors and their relevance for a specific segment. There's a possibility these insights help organizations in such segment to focus on conditions for the relevant factor(s), leaving out the effort of measuring a specific context in advance of a campaign or security program.

REFERENCES

Acuña, D. C. (2016). Effects of a Comprehensive Computer Security Policy on Computer Security Culture. *MWAIS 2016 Proceedings*, *10*.

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security*, *26*(4), 276–289.

Andersen, P. W. (2001). Information Security Governance. *Information Security Technical Report*, *6*(3), 60–70.

Avey, J. B., Avolio, B. J., Crossley, C. D., & Luthans, F. (2009). Psychological ownership: Theoretical extensions, measurement and relation to work outcomes. *Journal of Organizational Behavior*, *30*, 173–191.

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

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, *39*(PART B), 447–459. Elsevier Ltd.

Cheong, L. K., & Chang, V. (2007). The Need for Data Governance : A Case Study. *ACIS 2007 Proceedings*, (2005), 999–1008.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology*.

Cupoli, P. (2014). *DAMA-DMBOK2 Framework*.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*, 643–658. Retrieved from www.palgrave-journals.com/ejis/

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*, 79–98.

Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, *27*(4), 377–383. Elsevier Inc.

Van Dyne, L., & Pierce, J. L. (2004). Psychological ownership and feelings of possession: Three field studies predicting employee attitudes and organizational citizenship behavior. *Journal of Organizational Behavior*, *25*(4), 439–459.

Educause. (2009). *Data Stewardship, Security, and Policies*.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*. *Addison-Wesley Pub. Co*.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236.

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. Elsevier B.V.

Hoogervorst, J. A. P. (2009). *Enterprise governance and enterprise engineering*. *The Enterprise Engineering Series*.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95. Elsevier Ltd.
Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. Elsevier B.V.
Johnston, A., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129.
Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*(3), 549–566.
Johnston, A., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113–134.
Karwowski, W., & Glaspie, H. W. (2018). Human Factors in Information Security Culture: A Literature Review. *Advances in Intelligent Systems and Computing*, *July*.
Knapp, K. J., Morris, R. F., Marshall, T. E., & Anthony, T. (2009). Information security policy : An organizational-level process model. *Computers & Security*, 1–16. Elsevier Ltd.
Lee, Y. W., & Strong, D. M. (2003). Knowing-Why About Data Processes and Data Quality. *Journal of Management Information Systems*, *20*(3), 13–39.
Likert, R. (1932). A technique for the measurement of attitudes. *Archives of psychology*.
Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*.
Mayhew, M. G., Ashkanasy, N. M., Bramble, T., & Gardner, J. (2007). A study of the antecedents and consequences of psychological ownership in organizational settings. *The Journal of social psychology*, *147*(5), 477–500.
Mears, L., & Von Solms, R. (2007). *Corporate Information Security Governance : a Holistic Approach*.
Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. *Human Resource Management Review*.
Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311.
Mosley, M. (2008). DAMA DMBOK Functional Framework. *DAMA-DMBOK*, *3.02*, 1–19.
NEN-ISO-27001. (2013). *Nen-iso/iec 27001:2013*.
NEN-ISO-27002. (2013). *Nen-iso/iec 27002:2013*.
Olckers, C. (2013). Psychological ownership: Development of an instrument. *SA Journal of Industrial Psychology*, *39*(2), 1–14.
Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a theory of psychological ownership in organizations. *Academy of Management Review*, *26*(2), 298–310.
Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology*, *7*(1), 84.
Ponemon Institute. (2014). *2014 Cost of Data Breach Study : Global Analysis*. Retrieved from http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/
Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers and Security*, *23*, 638–646.
Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757–778.
Ryan, R., & Deci, E. (2000). Self-determination theory and the facilitation of intrinsic motivation. *American Psychologist*, *55*(1), 68–78.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145–147.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Siponen, M., & Vance, A. (2013). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289–305. Nature Publishing Group.

Sohrabi Safa, N., Solms, R., & Furnell, S. (2015). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82.

Von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security*, *25*(3), 165–168.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, *34*(3), 503–522.

Stanton, J. M., Stam, K. R., Guzman, I., & Caledra, C. (2003). Examining the linkage between organizational commitment and information security. *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Management and Cybernetics.*, *3*.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*, 255–276.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(December), 441–469.

Urdan, T. C. (2010). *Statistics in Plain English*. Routledge.

Veiga, a. Da, & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372.

Weber, K., Otto, B., & Osterle, H. (2009). One Size Does Not Fit All — A Contingency Approach to Data Governance. *ACM Journal of Data and Information Quality*, *1*(1), 4:1-4:27.

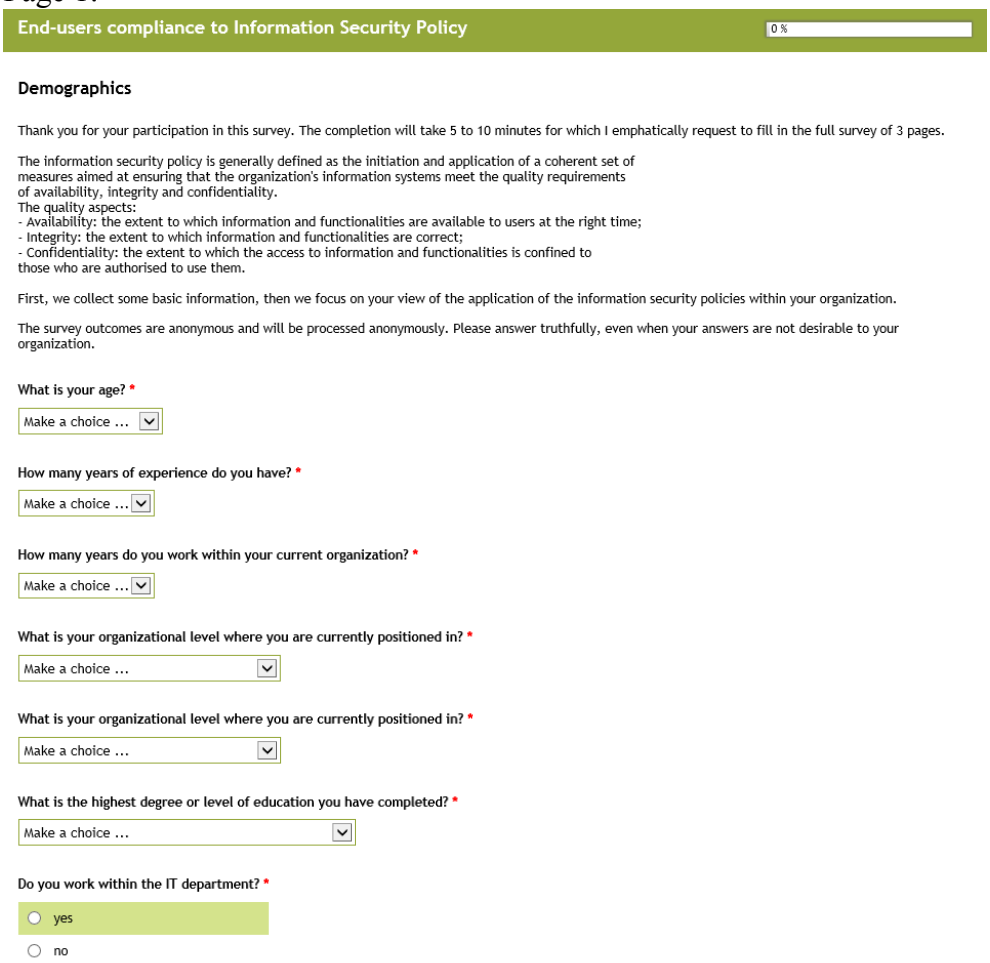
Willison, R., & Warkentin, M. (2013). Beyond Deterrence: an Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2).

APPENDIX A

The international version of the research instrument (in English) is provided below:

Page 1:



End-users compliance to Information Security Policy

0 %

Demographics

Thank you for your participation in this survey. The completion will take 5 to 10 minutes for which I emphatically request to fill in the full survey of 3 pages.

The information security policy is generally defined as the initiation and application of a coherent set of measures aimed at ensuring that the organization's information systems meet the quality requirements of availability, integrity and confidentiality.
The quality aspects:
- Availability: the extent to which information and functionalities are available to users at the right time;
- Integrity: the extent to which information and functionalities are correct;
- Confidentiality: the extent to which the access to information and functionalities is confined to those who are authorised to use them.

First, we collect some basic information, then we focus on your view of the application of the information security policies within your organization.

The survey outcomes are anonymous and will be processed anonymously. Please answer truthfully, even when your answers are not desirable to your organization.

What is your age? *

Make a choice ...

How many years of experience do you have? *

Make a choice ...

How many years do you work within your current organization? *

Make a choice ...

What is your organizational level where you are currently positioned in? *

Make a choice ...

What is your organizational level where you are currently positioned in? *

Make a choice ...

What is the highest degree or level of education you have completed? *

Make a choice ...

Do you work within the IT department? *

- yes
- no

Page 2:

End-users compliance to Information Security Policy

33 %

Research on Information Security Policy (page 2 of 3)

Page 2 of 3:
In this part, please indicate whether you agree or disagree with the statements about the information security policy within your organization. Choose the answer position you find most applicable to your situation or opinion.

Use the following principles in answering the statements:
- As an end user you have a kindly approach, there is no sense of evil.
- An information security policy is always present. This may not be formally identified, but may also consist of informal understandings, norms / values, your sense of discretion.

The information security policy of your organization *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am familiar with the current information security policy of my organization	○	○	○	○	○
I think the current policy is appropriate for my organization	○	○	○	○	○
The resources provided by my organizaion in order to carry out my work, allow me to perform my duties in accordance with the policy.	○	○	○	○	○
It takes more time to perform my work duties in accordance with the information security policy.	○	○	○	○	○
It takes more effort to perform my work duties in accordance with the information security policy.	○	○	○	○	○
Getting my job done comes before information security	○	○	○	○	○

What is your expectation on the effectiveness of an information security policy *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Each employee can make a difference in the security of the information systems of my organization	○	○	○	○	○
I can make a difference in the security of the information systems of my organization	○	○	○	○	○

Assess the role of your work environment in relation to compliance with the information security policy *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
My board thinks I should follow the information security policies of the organization	○	○	○	○	○
My immediate supervisor thinks that I should follow the information security policies of the organization	○	○	○	○	○
My colleagues think that I should follow the information security policies of the organization	○	○	○	○	○
The I(C)T department thinks I should follow the information security policies of the organization	○	○	○	○	○
The staff officers and advisors in my organization think that the information security policy should be followed	○	○	○	○	○
I believe other employees comply with the organization IS security policies.	○	○	○	○	○
It is obvious that the majority of employees comply with the organization IS security policies to help protect organization's information systems.	○	○	○	○	○
I am sure that other employees comply with the organization IS security policies.	○	○	○	○	○

Assess your intentions to follow the security policies of your organization *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am likely to follow organizational security policies	○	○	○	○	○
It is possible that I will comply with organizational IS security policies to protect the organization's information systems	○	○	○	○	○
I am certain that I will follow organizational security policies.	○	○	○	○	○

Page 3:

End-users compliance to Information Security Policy

67 %

Research on Information Security Policy (page 3 of 3)

Page 3 of 3:
In this part, please indicate whether you agree or disagree with the statements about the information security policy within your organization. Choose the answer position you find most applicable to your situation or opinion.

Again, use the following principles in answering the statements:
- As an end user you have a kindly approach, there is no sense of evil.
- An information security policy is always present. This may not be formally identified, but may also consist of informal understandings, norms / values, your sense of discretion.

Assess the role of ownership in compliance with the information security policy *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I feel I have a strong bond with the organization	○	○	○	○	○
I feel comfortable within the organization	○	○	○	○	○
I possess the competences to perform my job well	○	○	○	○	○
I feel the need to protect my information from use by others in the organization	○	○	○	○	○
I feel the need to protect my organization's information for use by other organizations	○	○	○	○	○

Assess the role of governance in following up the information security policy (see definitions below) *

NOTE: In the following questions two definitions are used:
'Data Steward' is a role in the organization which is responsible for the content of the information, including aspects such as quality and confidentiality.
'Data Custodian' is a role in the organization which is responsible for the technical aspects surrounding the storage of information such as the management of the storage systems.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The existence of a functional role such as a 'Data Steward' helps me to protect my organization's information	○	○	○	○	○
I think a distinction between the owner and the 'Steward' of information is important	○	○	○	○	○
The formalized existence of a functional role 'Data Custodian' helps me to protect my organization's information	○	○	○	○	○
I think a distinction between the owner and the 'Custodian' of information is important	○	○	○	○	○
The existence of a classification system for information (e.g. public, classified, secret) helps me to protect information	○	○	○	○	○
I think it should be clear what kind of information falls in a certain classification level	○	○	○	○	○
I think the consequences of assigning a particular classification should be clear	○	○	○	○	○

Press DONE at the bottom of this page to store the results.

I want to thank you for your cooperation!