Research Thesis
for the
Masters of Informatics

“Promote end-users compliance to the Information Security Policy”

Name: Peter Straver
Date: 23 September 2015
Supervisor: dr. Bas van Gils

ABSTRACT

This thesis document is the result of research conducted by Peter Straver in culmination of the Master of Informatics in the field of Information Management. The research is supervised by dr. Bas van Gils.

Business information, held within information systems, is critical for most organizations. To protect these critical information assets, security controls should be deployed which might come as a hindrance for the end-users, on top of other demands in their work. The Information Security Policies (ISP) give direction to their behaviors. Conditions can be shaped by organizations likely to promote so-called motivational factors influencing the end-users intentions to perform the desired behavior of compliance to the ISP in order to protect these information assets.

In the research documented in this thesis document, the applicable motivational factors are determined from literature, judged and refined by Subject Matter Experts. A survey is conducted within five contexts, within five different sectors. From the statistical analysis, findings are reported and conclusions on the hypothesis are drawn, which provide additional insights in this field of research. Also recommendations and suggestions for future research are reported.

In total, six motivational factors are found, applicable to intentions on compliance. From the research is learned, that the degree to which these factors relate differs per factor and per context. Two of these factors were found to always relate in such degree to compliance intentions that even without measuring the degree for a particular organization, applying these factors can be very effective for any organization or context. The other four factors have shown to be effective within particular context(s), meaning measurement of the context is needed, before utilizing these factors within an organization.

To measure such context this thesis delivers an research instrument –ready to use in practice- in the appendixes of this document.

This thesis therefore contributes to both research and practise. For research, additional insights on the motivational factors are reported in the thesis. It contributes to practice as well from the learnings on how to conduct such research in practice and for each conclusion reported, suggestions are listed on how to utilize a specific motivational factor in practice, within an organizational context.

ACKNOWLEDGEMENTS

In my opinion, completing my study, has only been possible with the support of a wide variety of persons surrounding me. The most important of all is, without any doubt, my wife Karen, supporting me from the pre-phase back in 2012 and the start of the study in 2013 until today, finishing my Master's thesis during our vacation in France. She is the one supporting and encouraging me every day, for the past years and on, to keep up with the study. Helping me to find the right combination between study, work and our private life, keeping the balance between it all. She and my son Wouter made the private time became quality time whenever I had the possibility to join them, mostly without complaining on me leaving to the attic again, where my home office is situated, finding me behind computer screens or books. I owe thanks to my parents and parents-in-law, as well as other family and best friends, for taking care of my beloved ones, whenever needed and especially for all the evenings I spend at HU and Karen needed help at home.

Besides them a big thanks goes to Bob, my former line manager, for helping me selecting this study and convincing the management team of Motiv to support and, also an important aspect, fund me on this study. Also during the moments where the balance was lost because of unforeseen happenings in work or private life, they kept supporting me and let me prioritize study and work efforts to my convenience.

I remember the first meeting of Cohort Sep'13 as it was yesterday, starting with the students introducing themselves and finding nicknames to remember each other's name. Within weeks we became a strong team of peer students supporting each other to reach our goals. During each of the six 'skillsday', guided by my coach Regine and Menda we came closer to each other and developed our soft-skills as well, which I find an important competence. In February 2015, during 'International Orientation' in Luxemburg most of us further developed our research questions with the help of Raymond, Anita and Erik and started to work on our proposal.

My luck was to find Bas as my thesis supervisor and combined with the support of Kobus' lectures and Jorien from the Program Office I managed to get the thesis proposal finalized. 'A good start is half of the work' is one thing Bas is very convinced of, as I discovered creating the proposal. In the end I'm very thankful to him, stressing me to the maximum during the proposal phase to deliver a high level of rigor in the proposal, forming a firm base for this thesis. This helped me a lot to keep track and overcome the stress during the thesis phase especially during my lobby for contexts to participate in the research because both pre-selected organizations rejected from the research. Main reason to reject was the timing of the research.

Ending up with no organizations about three weeks prior to the planned conduct of the final research was, mildly expressed, a somewhat uncomfortable situation. After pulling myself together I requested more than 25 contacts whether they might be interested in participation. After a few days of time-consuming lobbying around current and past business contacts using all possible channels I ended up with four contexts, within four different sectors willing to participate in the research! Therefore I thank Jan, Jeroen, Rob and Gerrit-Jan as my entrance point to the four contexts, where they convinced their board to participate in the research.

This thesis document is formed with the help of the subject matter experts Ronald, Jan and Michael and the review capabilities of Rohald and Jos, which all spend several hours participating in sessions or reviewing and commenting my work.

Not all of you could be mentioned in this paragraph, so for all other family, friends and professional peers: Thank you on supporting me, always being interested to listen to my elaborations on the study and thesis. I'm planning to finalize my study within weeks now, so let's bring back the social life…

Peter Straver, 5 August 2015.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Introduction

Following the guidelines of design-science research (Hevner, March, Park, & Ram, 2004) this thesis called "**Promote end-users compliance to the Information Security Policy**" started from the concept that several motivational factors can be used in order to influence the intentions of end-users to comply with their applicable Information Security Policy (ISP). The problem is: "**Which to use?"**

The thesis gives answer to the question: **What motivational factors relate, in which degree, to intentions on compliance and how could these insights be utilized to promote end-users compliance to ISP within a given organization?**

From the expectation / hypothesis that several motivational factors have a positive influence on intentions to comply, the thesis follows a 4 step approach:

1) Research on what motivational factors exist and are relevant to ISP compliance
2) Research on what method can be used to determine these relationships and their strength between these motivational factors and end-users intentions on compliance
3) Determine how these motivational factors relate to each other within a given organization
4) Report what can be learned from these insights in order to more effectively utilize these motivational factors within a given organization in order to promote end-users compliance to ISP

Research took place within 5 organizational contexts:

Context 1: Company in the business of ICT Security
Context 2: Healthcare Consultancy and Insurance company
Context 3: Marketing Technology company
Context 4: Retail company
Context 5: Financial Services company

Where the following relevant motivational factors are recognized from the research to influence compliance:

- Information Security Governance including 'Data Governance' and 'Information Classification'
- Social Pressures including 'Normative beliefs' and 'Peer behavior'
- Sense of ownership
- Effect of actions

1.1 Rationale

As a Security Architect I am confronted with companies struggling to keep their shields up on a technical level and wondering why their end-users still don't comply to the Information Security Policy (ISP) over and over. My practical experience has given me some feeling on the users intention to comply with the policy, especially when they are personally involved with the information and have insight in the way information security governance is organized within their organization.

More than technical means is needed to solve these information security related problems in a company. To be able to monitor compliance to relevant information security policies, any information security manager should be empowered with measurement tools (Von Solms & Von Solms, 2004).

1.2 Contribution

This thesis is intended to contribute to both research and practice in information systems security. Within the context of research this thesis provides additional insight into the following topics:

1. Information Security Governance
2. Sense of ownership
3. Social Pressures
4. Effect of actions

These topics including some control variables are researched in their relation to the intention of the end-user to comply to the ISP. The thesis designs a method to gain insight in motivational factors relevant to policy compliance within a given organization. These motivational factors are likely to encourage greater commitment in protecting organizational information if they have a personal meaning or are of interest to the end-users.

There's less research on non-malicious behavior in contrast with malicious behavior, suggesting the focus of existing research is found to be mostly on intentional abuse. The goal of this thesis is to provide more insight in the less researched roles of ownership and governance 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.

Encouraging and motivating end-users behavior is a challenge faced by (chief) security officers and other IT security managers (Warkentin & Johnston, 2008). Also in ISO 27002 (2013), recognized as an industry best practice, it is stated that compliance with the ISP and all relevant legislation and regulations concerning the protection of corporate information and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible. The outcomes of this thesis are of great value for such individuals giving them insights to complement their controls. The outcomes also provide more general benefits for companies and society by adding to the insight on intentions to comply to the ISP.

1.3 Lay-out of thesis document

The background / context of the thesis is described in the next chapter. From a defined problem statement, research questions are subtracted. To answer these questions a 4 step research design approach is followed including, amongst others:

- Literature review and conceptual model design
- Research instrument (survey) design
- Conducting the survey
- Analyze the outcomes and report findings, conclusions and recommendations

These process steps are captured in a process step flow diagram which is shown in chapter 5 which guides the reader through the rest of the thesis document.

The article about this research, being part of the thesis-phase, is found in Appendix H (Article).

2 Background / Context

This chapter describes some background and context around the subject of the thesis to give insight in the needs to protect business information and the role end-users have in this challenge faced by any organization nowadays.

2.1 No information – No business

Business information plays an important role for most organizations (Ifinedo, 2014). To compete in today's business environment, organizations rely heavily on information systems (IS). The protection of the business information held in such information systems has emerged as a key managerial priority (Ifinedo, 2014; NEN-ISO-27002, 2013). This thesis focusses on information held in IS, but some theoretic parts and outcomes might also be applicable to non-digital information as well.

Johnston and Hale (2009) state that organizations are constantly threatened within the modern 'hyper-connected' business landscape. There are still many firms that operate ineffective information protection programs, where the ineffective protection can often be attributed to the reactive approach to information security planning. Their strategies are based on incidents (Johnston & Hale, 2009). Organizations need security controls to proactively protect their valuable information, considering today's threatened cyber environments (Knapp, Morris, Marshall, & Anthony, 2009; Kritzinger & Smith, 2008).

In order to protect the critical information systems and its business information assets, organizations often deploy security techniques. These techniques and tools are rarely sufficient in providing protection of business information. Research has indicated that a failure to focus on the individuals working with the business information assets, alongside the technology based solutions, leads to failure in efforts to prevent security incidents and breaches. (Guo, Yuan, Archer, & Connelly, 2011; Ifinedo, 2014)

Business information, held within information systems (IS), is critical for most organizations;

Today's 'hyper-connected' business landscape threatens organizations critical assets;

2.2 Threat formed by employees

"Information security, which involves preserving the confidentiality, integrity and availability of business information, helps to mitigate the various risks to such information through the application of a suitable range of security controls. A suitable range of security controls could be defined as having an appropriate mix of physical, technical or operational security controls." (Posthumus & Von Solms, 2004)

Different recent publications mention the role of the users who need to be able to "access information anywhere, anytime, and from a range of different devices" (CA Technologies, 2014) and a shift in the management of users and their role in security is observed. One outcome of the yearly 'Data Breach Investigation Report', published by Verizon states that nearly every incident involves some element of human error (Verizon, 2014a) and that this risk is found wherever trust is placed in people within a business (Verizon, 2014b). "Many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security." (Bulgurcu, Cavusoglu, & Benbasat, 2010)

Ponemon Institute (2014) found in their year 2014 research on the cost of data breaches at 314 organizations that 30% of the root causes for data breaches concerned employees or contractors abuse. Despite this recognition of human error as a serious threat, only 11% of budget is allocated to dealing with malicious or negligence (non-malicious) insiders or third parties. Negligent insider risk (8,2% of total risk) is even rated higher than malicious insider risk (6%) (Ponemon Institute, 2015).

These publications are supported by empirically validated research where a serious threat to the organization is seen to be formed by employees, not adhering to the information security policies (Siponen, Mahmood, & Pahnila, 2009). Hindrance caused by security practices is one of the reasons employees dislike such practices (Herath & Rao, 2009a).

To protect these critical assets, a suitable range of security controls should be deployed;

For the end-users these controls come as a hindrance, on top of the other demands in their work;

2.3 Promote end-users behaviors with their intent to comply with policy

It is recognized that one approach for making information security effective within organizations is to promote good end-user behaviors and constrain bad end-user behaviors (Stanton, Stam, Mastrangelo, & Jolton, 2005). To give direction to these behaviors a necessary foundation is found in ISP to define the concepts of information security (Knapp et al., 2009; Mears & Von Solms, 2007). The ISP should be 'translated' into procedures that will positively affect the attitude and behavior of employees (K. Thomson & Solms, 2006). Even if an ISP is in place to help safeguard an organization against the misuse, abuse and destruction of information systems assets, its employees often do not readily comply with such policies. A beneficial approach to compliance requires organizations to focus on their own employees' intentions and behaviors towards compliance to the ISP (Ifinedo, 2014).

"A central factor in the theory of planned behavior (TPB) is the individual's intention to perform a given behavior. Intentions are assumed to capture the motivational factors that influence a behavior; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behavior. As a general rule, the stronger the intention to engage in a behavior, the more likely should be its performance." (Ajzen, 1991)

Summarized; Within a context of information security, conditions can be shaped by organizations likely to promote motivational factors influencing the individual's intentions to perform desired behavior (Ajzen, 1991; Ifinedo, 2014; Ryan & Deci, 2000a; Stanton et al., 2005; Weber, Otto, & Osterle, 2009).

Good end-users behaviors should be promoted and bad end-users behaviors constrained;

2.4 Focus on non-malicious end-users compliance

What good are policies and guidelines if non-malicious end-users do not comply with the Information Security Policy (ISP) of a company? (Ifinedo, 2012).

The focus of the thesis is on motivational factors that influence the intention of non-malicious end-users to comply with the ISP of an organization. That area of research is also explored by Siponen et al. (2009) as well as Herath and Rao (2009b) and others. The choice of the focus area lies both within my personal interest, as well as my professional work as Security Architect at a company in the business of IT security sourcing. That company can be defined as a Managed Security Services Provider (MSSP). Zhao, Xue and Whinston (2009) define MSSP as "a provider of a range of security services", to induce more efficient allocation of security resources because the MSSP internalizes the externalities of security investments between their member firms.

Information Security Policies (ISP) give direction to these behaviors;

2.5 Different roles have conflict of interest

In an organization it's often the responsibility of the 'security manager' to encourage end-users, at all levels of the organization, to act in a manner to protect the organizations' information systems and assets. Therefore, the security manager, or such equal role, should communicate the importance of information security in an intelligible manner to all members of the organization. For the users this comes on top of the other demands they are faced with in their everyday work (Albrechtsen & Hovden, 2009). Employees do not comply with ISP because they:

- perceive that their workload is high
- they are busy with other assignments
- security policies slow them down
- other work is more important

(Siponen & Vance, 2010).

This conflict of interest is illustrated in Figure 1.

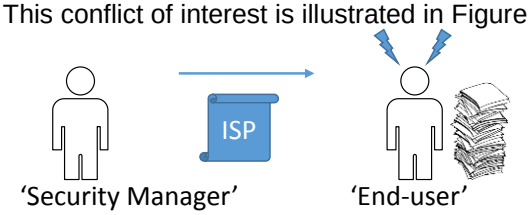


Figure 1 Conflict of interest

The different roles within organizations have a conflict of interest;

2.6 Violation of ISP

ISP is always present within organizations. The security manager should understand, account for and address both the formal and informal organization parts (von Roessing, 2010). A formal ISP is typically a document that outlines specific requirements or rules that must be met. It is formal when it is explicitly defined or stated (Ifinedo, 2014). There also exists an informal part within the organization in which things may operate outside of, or without, written policies (von Roessing, 2010). In the informal part the ISP's are implicitly stated (Ifinedo, 2014).

There is a distinction between ISP 'violation' (not complying to ISP) and general computer 'abuse' (Siponen & Vance, 2013). These are explained in Figure 2 where the continuum of Willison & Warkentin (2013) distinguishes between non-deliberate or deliberate. In the case of non-deliberate violations the end-users might violate ISP only because they are unaware of the ISP of their organization (Siponen & Vance, 2013). *"In contrast, in the case of deliberate violations, employees are aware of the ISP, but choose to violate the ISP anyway, either maliciously or non-maliciously"* (Siponen & Vance, 2013).

The focus of this thesis is on the non-deliberate, non-malicious end-users which are in some extend aware of the ISP whether formally of informally stated, being the upper 2 categories within the continuum. This is because the last group (malicious abuse) is less influenced in their behavior using ISP (Siponen, 2001; Stanton et al., 2005).

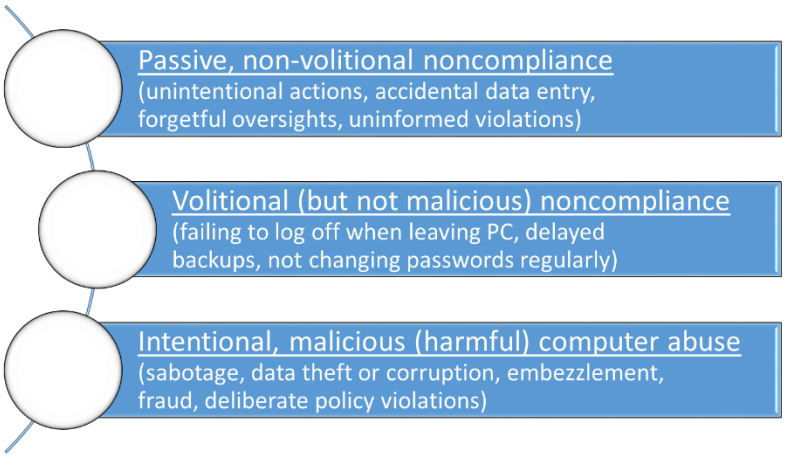


Figure 2 Continuum of ISP violations from Willison & Warkentin (2013).

Despite ISP, end-users often do not readily comply with such policies;

2.7 Shape conditions to promote good behavior

As shown in Figure 3; organizations can shape conditions likely to promote two types of motivations influencing the intentions of the end-users (Amabile, 1993; Ryan & Deci, 2000a, 2000b). “Extrinsic motivation focuses on the goal-driven reasons, e.g. rewards or benefits earned when performing an activity, while intrinsic motivation indicates the pleasure and inherent satisfaction derived from a specific activity. Together, extrinsic and intrinsic motivation influence an individual’s intentions regarding an activity as well as their actual behaviors” (Lin, 2007).

In the end, the individual’s intentions should lead to the desired behavior of compliance to the ISP which in turn leads to an increased level of protection of the organization’s information and technology resources (Bulgurcu et al., 2010).

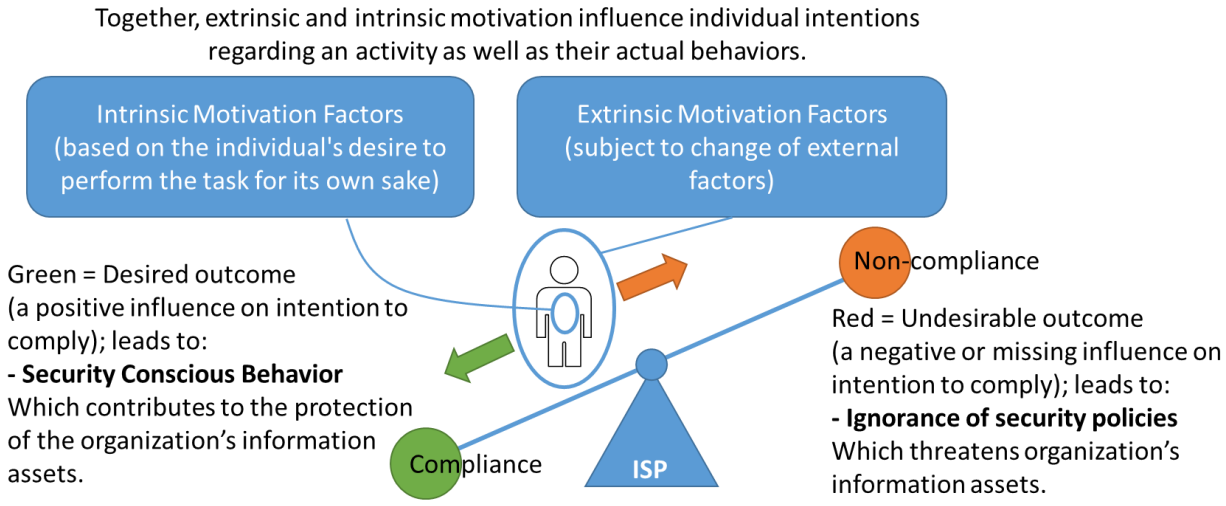


Figure 3 Promote 'good behavior'

2.8 Handling organizations assets; the company car example

Handling organization's information could be compared to handling any other organization's asset, for example a 'company car' asset which is assigned to an employee. In this car example one can imagine several motivational factors might influence such employee in his or her intention to follow up on the corporate policies regarding the use of that car in order to protect the asset.

On the one hand formal policies on the use of company owned vehicles explicitly express some controls such as: "You must conform to all traffic laws, signals, and markings, and make proper allowance for adverse weather and traffic conditions", to regulate the intentions of the employee and prevent misuse. On the other hand the company also relies on more informal and implicit due diligence of the employee in handling the asset given into use. It is important to mention that "conventional wisdom suggests that people will take better care of, and strive to maintain and nurture the possessions they own." (Avey, Avolio, Crossley, & Luthans, 2009) making sense of ownership of the asset a part in the protection of the asset as well.

In the example of the company car the explicitly expressed controls fall in the category of extrinsic motivational factors while the implicit controls e.g. 'sense of ownership' fall into the category of intrinsic motivational factors. Both intrinsic and extrinsic motivational factors influence the individuals intentions to perform desired behavior, namely taking 'good care' of the company car.

2.9 Organizations context

Back to organization's information, which is a vital asset for most organizations (K. Thomson & Solms, 2006). As in the case of the company owned vehicle, also for the company owned information, according to Thomson and Solms (2006), most organizations rely on an explicit ISP, in which the vision of senior management with regard to information security is explicitly outlined and 'translated' into procedures that will positively affect the intentions and behavior of employees. The same parallel can be made in an implicit manner; "Eventually the de-facto, or second-nature, behavior of employees should adhere to the behavior necessary to adequately protect the information assets of an organization" (K. Thomson & Solms, 2006).

From the research of Ajzen (1991) is learned that any single sample of behavior reflects not only the influence of a relevant general disposition, but also the influence of various other factors unique to the particular occasion, situation, and action being observed. The remedy would be to aggregate specific behaviors across multiple organizations, by looking at broad, aggregated, valid samples of behavior, which is out of scope for a thesis research and makes the outcomes less applicable to practice (Ajzen, 1991; Siponen & Vance, 2013).

A second argument to perform the research within the context of a given organization has to do with corporate culture. Not only does corporate culture place constraints upon the activities and behavior of employees, it also prescribes what the organization and its employees must do (K.-L. Thomson, Solms, & Louw, 2006). Because every company has its own culture, the motivational factors to use in order to influence the intentions of end-users behavior differs between companies (Stanton et al., 2005).

Therefore the research of the thesis is designed to predict and explain human behavior within the specific context of a given organization (Ajzen, 1991).

3 Problem definition

Chapter 1 and 2 introduced the rationale and background for this thesis. Wrapping up all parts makes up the following summary:

Within a context of information security, conditions can be shaped by organizations likely to promote motivational factors influencing the end-users intentions on compliance to ISP in order to protect the organization's information they exchange in the digital domain.

Figure 4 shows the full context map for this thesis built from the parts found in the previous chapters.

3.1 Problem statement

From the context map the following problem statement is extracted:

Several motivational factors can be used in order to influence the intentions of end-users to comply with their applicable ISP.
The problem is: "Which to use?"

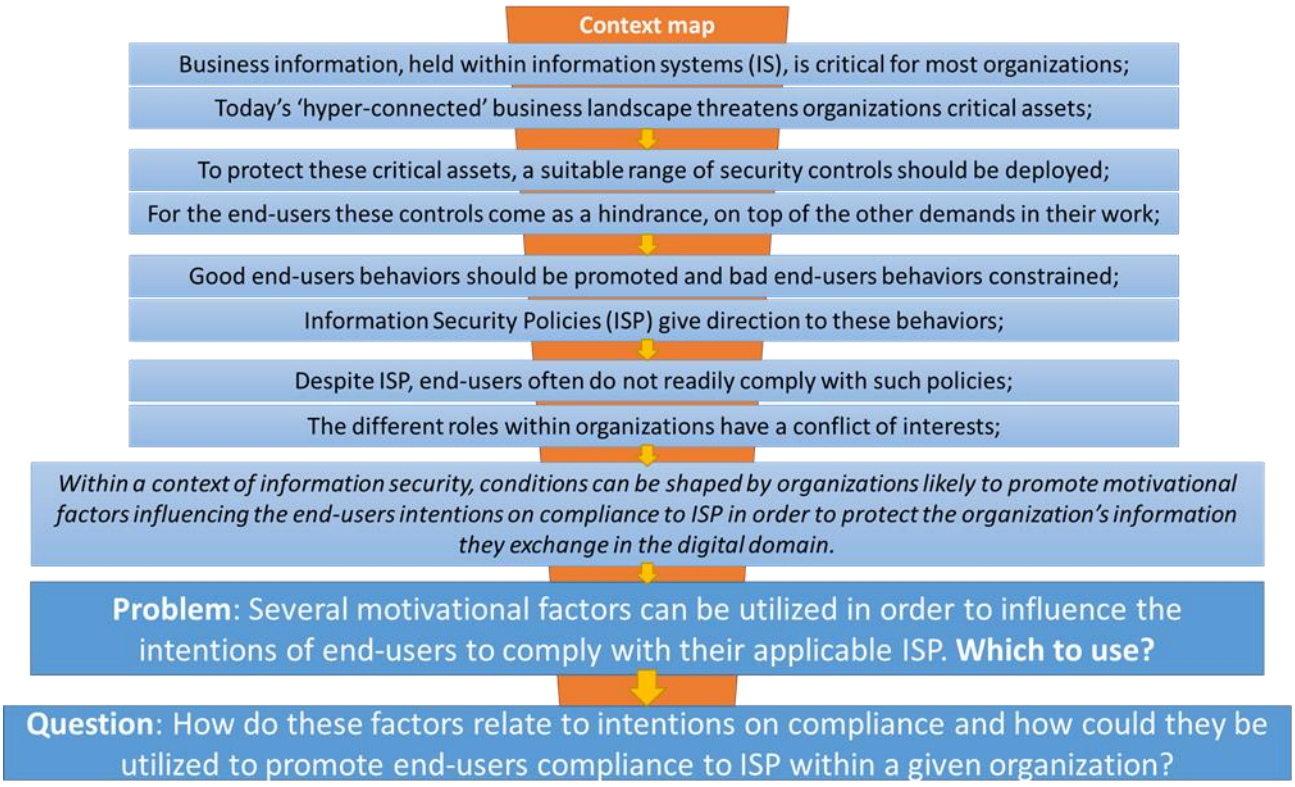


Figure 4 Context map

4 Research questions

To answer the question “Which to use?” it is needed to know how these factors relate to intentions on compliance within the context of a specific organization in order to effectively utilize the motivational factors within that organization to promote compliance of end-users to ISP. The following research question is formulated to research this question:

What motivational factors relate, in which degree, to intentions on compliance and how could these insights be utilized to promote end-users compliance to ISP within a given organization?

The research question is answered in parts during the different steps within the research process, in the end leading to the answer on the research question as reported in chapter 19.

4.1 Sub-questions

The sub-questions making up the different steps within the research process are:

1) *What motivational factors exist and are relevant to ISP compliance?*
2) *What method can be used to determine the relationships and their strength between these motivational factors and end-users intentions on compliance?*
3) *How do these motivational factors relate to each other within a given organization?*
4) *What can be learned from these insights in order to more effectively utilize the motivational factors within a given organization in order to promote end-users compliance to ISP?*

Where it is expected to:

- ✓ Find relevant motivational factors and …
- ✓ a method to measure their relevance …
- ✓ in order to utilize these motivational factors …
- ✓ to effectively promote end-users intentions on compliance to ISP…
- ✓ in order to protect the organization’s information exchanged within the digital domain.

Chapter 5 expresses the research method and process to follow in order to answer the research question in more detail.

5 Research design & method

The thesis follows the process steps as depicted in Figure 5 to answer the research question.

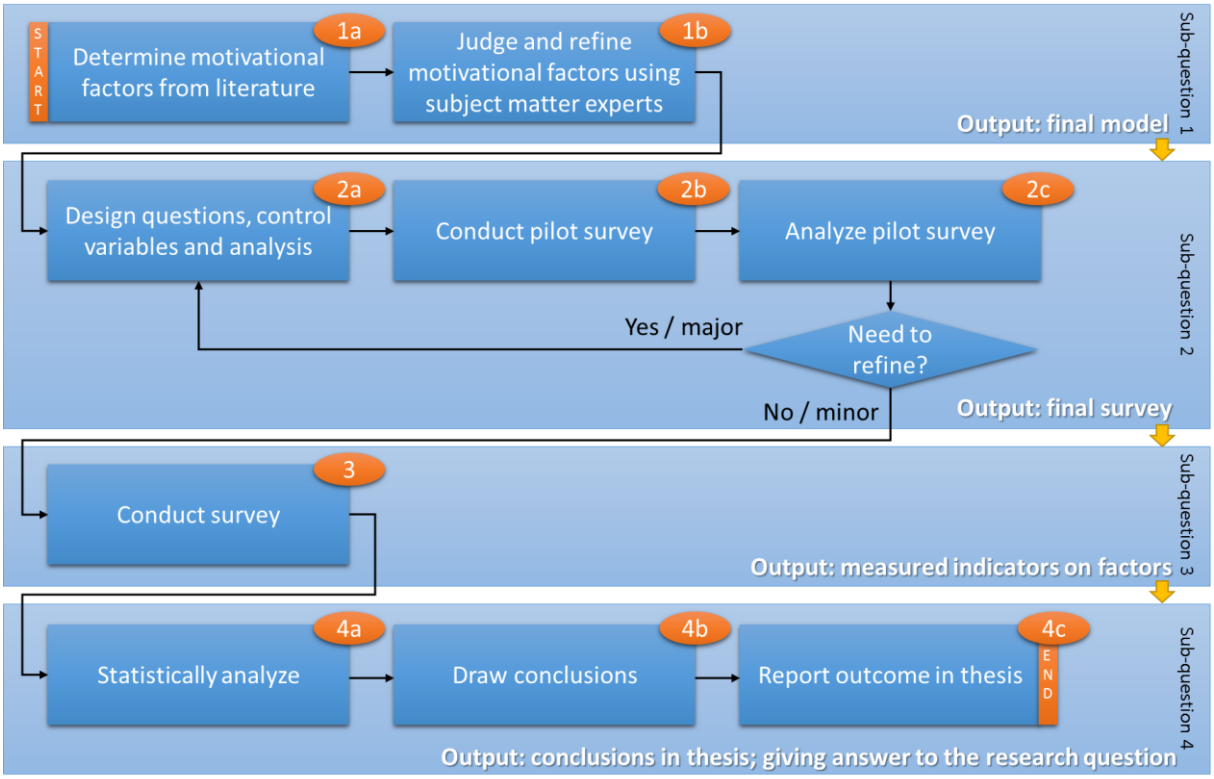


Figure 5 Process steps

The research methodology differs per sub-question and is described in the following sections. Each step is detailed in a separate part of the thesis as shown in Table 1.

Step	Page
Literature Review (Step 1a part 1)	20
Conceptual Model (Step 1a part 2)	26
Subject Matter Experts "Judge/Refine" (Step 1b)	29
Proposed Conceptual model of thesis (Output 1)	31
Survey design (Step 2a)	32
Pilot Survey + Analysis (Step 2b and 2c)	41
Analyze pilot survey (Step 2c)	43
Final survey instrument (Output 2)	50
Conduct Final Surveys (Step 3)	52
Measurements (Output 3)	57
Analysis (Step 4a)	58
Conclusion and Recommendations (Output 4)	75
Appendix G (Additional findings)	96

Table 1 Steps of thesis

5.1 Sub-question 1

Question: What motivational factors exist and are relevant to ISP compliance?

Method used:
The relevant motivational factors are determined from the literature review (chapter 6) leading to the conceptual model (chapter 7).

- The relevant motivational factors have been judged and refined using two informal 'Subject Matter Expert' (SME) review sessions by a total of 3 subject matter experts. Each of them is expert in his own field of work and they judged the theoretical framework of the thesis from experiences in their day-to-day jobs.
- This informal judgment had the goal to determine the variables are chosen correctly and can be measured as such in the survey.
- Also the learnings from Siponen & Vance (2013) as guidelines for contextual relevance of field studies in the case of ISP violations, were taken into account.

Output: Final conceptual model.

5.2 Sub-question 2

Question: What method can be used to determine the relationships between these motivational factors and end-users intentions on compliance?

Method used:
The motivational factors from the conceptual model were used to design the questions and control variables leading to the final survey instrument.

- The survey questions are based on survey questions found in Herath & Rao (2009b), appendix A (Survey instrument of validated research).
- Literature review for the other motivational factors is used to define the survey questions for the additional motivational factors.
- Defined survey questions were reviewed and tested by the SME's.
- A pilot survey is conducted on end-users of the corporate information systems from within a specific context.
    - Context 1: Dutch company in the business of ICT Security
        - (Motiv IT Masters B.V.).
- The results of the pilot survey are statistically analyzed.
- Based on the findings in the pilot survey the survey questions have been refined.

The pilot survey analysis did not lead to major refinements. Therefore the defined loopback for major survey refinement as shown in Figure 5 sub-question 2 could be skipped.

Output: Final survey to be conducted under target groups.

5.3 Sub-question 3

Question: How do these motivational factors relate to each other within a given organization?

Method used:
Following a process of cross-sectional quantitative research design using self-completion questionnaires of closed questions (Bryman & Bell, 2007).

- The survey was conducted on four target groups. Each target group represents a specific organization context. These contexts are described extensively in chapter 16.
    - Context 1 (conducted in pilot): Company in the business of ICT Security
    - Context 2: Healthcare Consultancy and Insurance
    - Context 3: Marketing Technology (Global context)
    - Context 4: Retail
    - Context 5: Financial Services
- For each context, the survey participation request is distributed by email using a fixed approach and using similar introduction statements.

Output: Measured values of motivational factors for all target group surveys, to be analyzed statistically as a total and per context.

5.4 Sub-question 4

Question: What can be learned from these insights in order to more effectively utilize the motivational factors within a given organization in order to promote end-users compliance to ISP?

Method used:

- The measured values have been statistically analyzed as described in chapter 12.
- Based on the relationships found and the knowledge on the theoretical relationships found in literature, conclusions are drawn.
- Outcomes are reported as conclusions and recommendations.

Output: Relevant results from statistical analysis and conclusions to answer the research question.

6 Literature Review (Step 1a part 1)

Within the scope of answering sub-question 1, the motivational factors are determined from literature and the applicable literature are summarized in the literature review. Next, the selected motivational factors are judged and refined using subject matter expert sessions.

The steps are outlined in Figure 6.

Figure 6 Steps in sub-question 1

Step 1a is split in 2 parts being the literature review (chapter 6) and the conceptual model (chapter 7).

6.1 Information Security Management

"News headlines in recent years have demonstrated the importance to the business of an effective approach to Information Security Management (ISM) by illustrating what can happen in its absence." (Clinch, 2009)

ISM preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed (NEN-ISO-27001, 2013). One example of what can happen in the absence of effective ISM is the case of the loss in transit of Her Majesty's Revenue and Customs (HMRC) child benefit records in the year 2007. In that case documented procedures were in place and would have prevented the incident, but staff were not aware of them (Clinch, 2009). The organization failed to express the importance of information security to all members of the organization (Albrechtsen & Hovden, 2009). Organizations must recognize that non-malicious insiders can inadvertently access and distribute sensitive information (Fyffe, 2008).

According to NEN:ISO standard 27002 (2013) organizations should develop organization-specific ISM guidelines. During development of these guidelines the specific information security risk of the environment should be taken in consideration (NEN-ISO-27002, 2013). Models can be used to quantitatively evaluate the value of business information assets, their vulnerabilities and the threats to those assets. The outcome of such evaluation can be used to determine appropriate risk treatment and select countermeasures that effectively reduce information security risks and answer the question: 'how much is enough?' (Bojanc & Jerman-Blažič, 2013; Gordon & Loeb, 2002).

6.2 Influence end-users intentions and behavior

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 ISM effects and solve behavioral issues, an understanding of what factors motivate employees to compliance is needed (Bulgurcu et al., 2010). The demonstrated relation between intention and actual behavior by Fishbein and Ajzen (1975) forms a starting point in researching such relationships.

In their research on end-users security behaviors Stanton et al. (2005) created and tested a six-element taxonomy of end-user security-related behaviors within two dimensions being intentionality and technical expertise. In the dimension of intentionality several mechanisms were found that may help to move end-user behaviors from the "naïve mistakes" category (behavior which requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources.) to the "basic hygiene" category (behavior

which requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources.).

To research such a positive move of end-users to a clear intention to comply to their ISP, the conceptual model of Herath & Rao (2009b) forms a foundation for this thesis to empirically test motivational factors positively influencing the end-users intentions to comply to ISP.

When researching a move of end-users intentions, also the integration of habit (a routinized form of past behavior) should be taken into account. An empirical test showed that end-user intention for current and future compliance is strongly reinforced by past behavior (habitual compliance). The results show that past and automatic behavior of end-users should be addressed in order to improve their current and future level of compliance (Vance, Siponen, & Pahnila, 2012).

Further research related to intentions to comply to ISP can be found in literature of Stanton et al. (2005) which, as already mentioned, created and tested a taxonomy of end user security-related behaviors. Their model and the focus area of the thesis and the 'positive move' is shown in Figure 7.

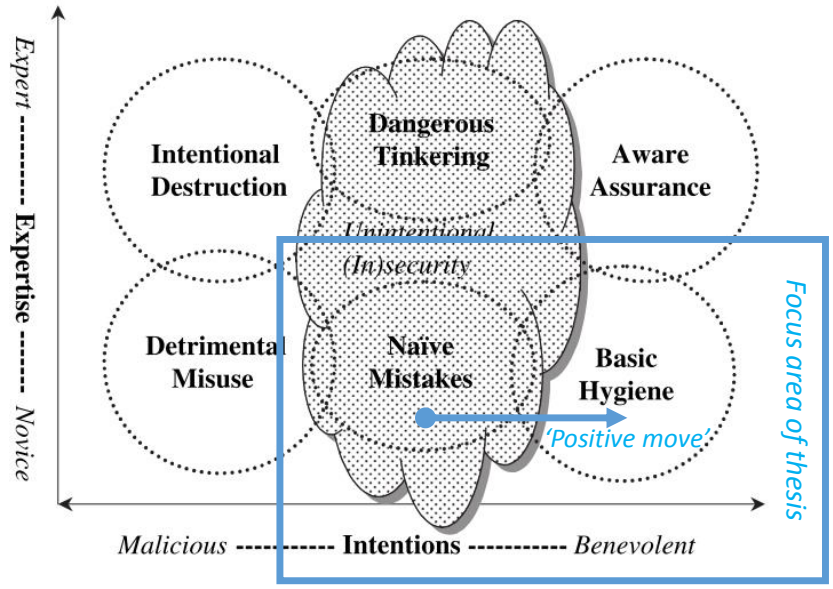


Figure 7 Taxonomy of end user security behaviors (Stanton et al., 2005)

Another base for the intrinsic and extrinsic motivational factors is found in Ryan and Deci (2000a), based on their Self-Determination Theory (SDT). “Perhaps no single phenomenon reflects the positive potential of human nature as much as intrinsic motivation, the inherent tendency to seek out novelty and challenges, to extend and exercise one's capacities, to explore, and to learn”. In contrast with intrinsic motivation they refer to extrinsic motivation as “the performance of an activity in order to attain some separable outcome”. (Ryan & Deci, 2000a). The resulting continuum and focus areas of the thesis is shown in Figure 8.

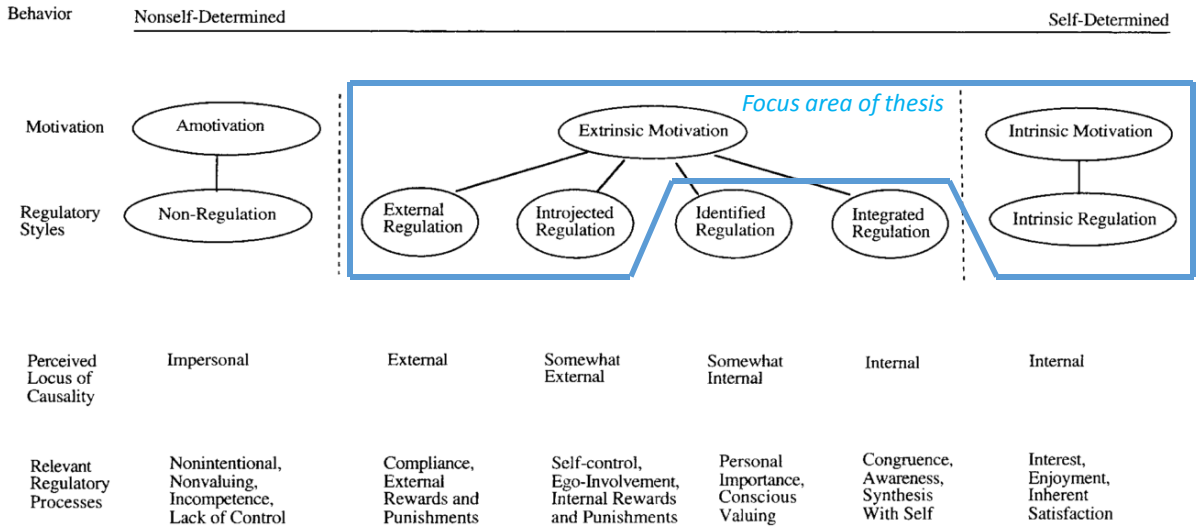


Figure 8 The Self-Determination Continuum (Ryan & Deci, 2000)

The different extrinsic and intrinsic motivational factors have a certain synergy as reported by Amabile (1993) which presented a foundation for a model of motivational synergy with several findings. Two mechanisms are proposed and discussed for certain combinations of intrinsic and extrinsic motivations (Amabile, 1993). This knowledge is important when drawing conclusions on the relationships found during the research of this thesis.

6.3 Overview of research areas on 'influencing behaviors'

One thing, perhaps unnecessary to mention once more, is the focus of the thesis on end-users which intent to behave non-malicious as defined in the dimension of internal, human perpetrator with an accidental intent, like acts by employees (Loch, Carr, & Warkentin, 1992). The same 1992 dimensions are still to be adapted, for example by Willison and Warkentin (2013) although their focus was on the opposite being intentional, malicious abuse. End-user behavior can be influenced in different ways (Stanton et al., 2005). Different research areas with a focus on influencing malicious and/or non-malicious behavior have been researched in the past years, for which an overview is presented in Table 2 below.

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

Table 2 Overview of literature

The next chapters elaborate on the research areas mentioned in Table 2;

6.3.1 Research area: 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 data security in which they involve end-users. The involvement of the end-users is relevant within this thesis as another conclusion of Straub is that articulation (in the sense of formalization) of the policy and actively enforce the policy leads to a benefit in information security. In the light of deterrence, the notion 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 in total contains four countermeasures being deterrence, prevention, detection and remedies. Their 'Countermeasures Matrix' used in context with their 'Security Risk Planning Model' form a principle to efficiently and effectively formalize parts of the security system where possible.

From D'Arcy et al. (2009) support is found that user awareness of security policies combined with monitoring (as a parallel to 'prevention' and 'detection' part of the before mentioned 'countermeasures matrix' (Straub & Welke, 1998)) have a deterrent effect on the intention to misuse IS. Sanctions are part of deterrence strategy and especially the perceived certainty and/or severity of these sanctions play a role towards the end-users.

6.3.2 Research area: 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 & Rogers, 1983). The purpose of the investigation was to examine the influence of fear appeals on behavioral intentions, specifically the compliance of end-users. They discovered an impact on the end-users behavioral intentions to comply to ISP when certain fear-inducing arguments come into play. Although 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 & Warkentin, 2010).

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

6.3.3 Research area: Neutralization

Neutralization, which includes different factors like 'defense of necessity' and 'denial of responsibility', is another factor of research in the policy compliance intention field of work. Neutralization is a prominent theory in the field of Criminology and is applied by Siponen & Vance (2010) in the context of IS. A theoretical framework is proposed to measure the effects of neutralization techniques alongside those of the sanctions described by deterrence theory. At developing and implementing organizational security policies and practices neutralization was validated to be a factor to take into account. Again, compliance intentions is the center of the proposed framework (Siponen & 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;
- disgruntlement as a result of perceptions of organizational injustice.

as three areas worthy of further empirical investigation. Thereby bringing to attention "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 & Warkentin, 2013). This question on the impact of emotions is taken into account in the intrinsic motivation part of the conceptual model for this thesis.

6.3.4 Research area: Ownership

Demontrated Ownership as in end-users participation to engage them in protecting sensitive information was investigated as factor to compliance. The data was collected in a questionnaire survey of 228 members of ISACA, the association behind DAMA DMBOK framework (2008), and mentions the users to be a resource to information systems security (Spears & Barki, 2010). This research is a primary source of the 'Data Ownership' factor in the conceptual model for this thesis 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 an company car, or in the focus of this thesis an organization's information asset covered by the organization's ISP. A conclusion of Pierce, Kostova and Dirks (2001) is that psychological ownership has emotional, attitudinal and behavioural 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 organisation is also likely to play a role in his/her engagement in security (Herath & Rao, 2009a).

6.3.5 Research area: Rationality and Awareness

Bulgurcu et al. (2010) sets focus to the same of this thesis which is non-malicious abuse and also the recognition that employees, being the end-users of the IS, can be great assets in the effort to reduce risk related to information security. In specific the rationality based factors behind an end-users drive to comply to policy is investigated. 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 formed by benefit and cost of compliance and the cost of non-compliance but also from the construct of information security awareness. Especially their first hypothesis is of special interest for this thesis where is stated: "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). They conclude their research with the finding of the key role of mediator that 'attitude' plays in explaining the relationships between information security awareness and the intention to comply.

6.3.6 Research area: Planned behaviour & Protection motivation

The model of Ifinedo (2012) fuses 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, thereby supporting Bulgurcu et al. More on attitude is researched by Guo, Tyan, Archer and Connely (2011) with a strong focus on end-user intentional and non-malicious actions, finding importance of linking security and business objectives by cultivating a culture of secure behavior in organizations.

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

6.3.7 Research area: Information Security Governance

"*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*." (Posthumus & Von Solms, 2004). Several governance themes are described by Hoogervorst (2009) which consist of 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.

7 Conceptual Model (Step 1a part 2)

The literature review in chapter 6 describes a collection of research area's which are recognized as applicable knowledge to the thesis. An important best practice in research is the development of a conceptual model providing a representation of the problem domain (Hevner et al., 2004) to be researched.

7.1 Base for conceptual model of thesis

The starting point of this thesis lies within the conceptual model of Herath & Rao (2009b) , as shown in Figure 9 below. That model has shown to be of great value to information security researchers. It 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 & Rao, 2009b).

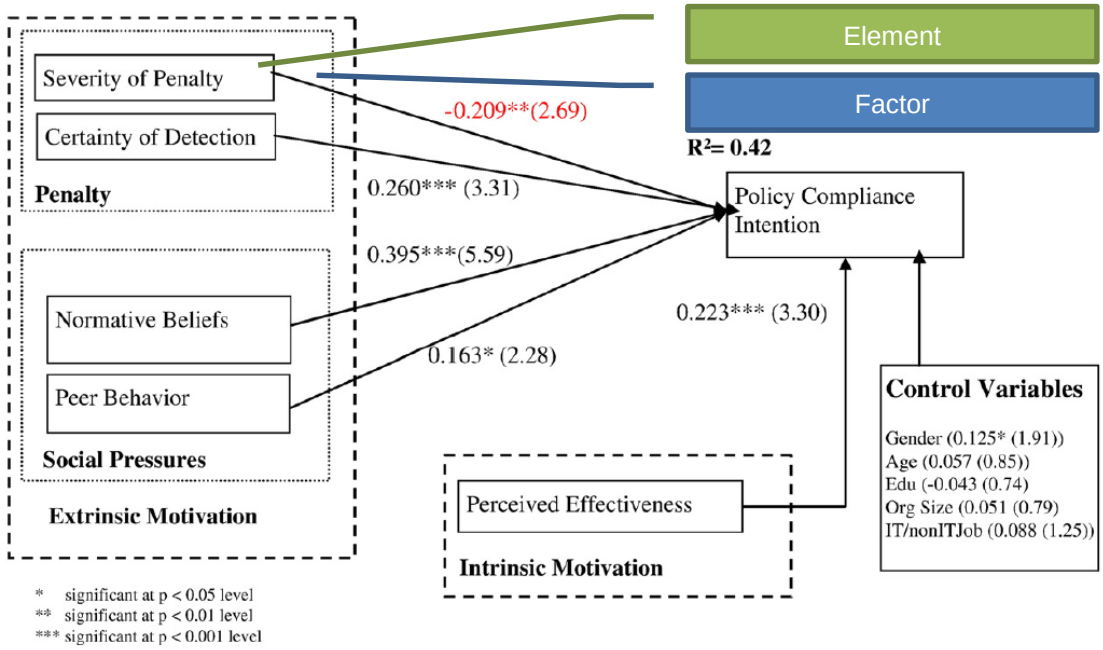


Figure 9 Herath & Rao (2009) conceptual model as a starting point

The model in Figure 9 contains one dependent variable (Policy Compliance Intention), being influenced by three factors containing a total of 5 elements forming the independent variables. To control whether other variables have an influence on PCI some control variables are in the model as well. Herath & Rao (2009b) conclude stating: "Our findings suggest that security behaviors can be influenced by both intrinsic and extrinsic motivators. Pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play a role in security policy compliance intentions".

The role of penalties remained unclear in the Herath & Rao (2009b) research. They found no support for the severity of penalties and found an unexpected effect in opposite direction as can be seen in Figure 9. It is suggested to further research the role of penalties in shaping behaviors (Herath & Rao, 2009b). Research on this factor should be self-contained because of the contradictory findings to get more insights on this specific factor before embedding these elements in a multi-factor model. Therefore the role of penalties is suppressed from the conceptual model of this thesis.

'Subjective norms', in the model stated as 'Normative Beliefs' are defined as the belief as to whether or not a significant person wants the individual to do the behavior in question (Herath & Rao, 2009a).

7.2 Additions to the base model; additional motivational factors

Extensive research has been conducted on the 'Policy Compliance' field of knowledge for which a summary is provided in chapter 6 of this proposal. Several factors surrounding compliance to such ISP have been researched in relation to policy compliance, for example in the area of deterrence (Straub, 1990), fear (Johnston & Warkentin, 2010) and neutralization (Siponen & Vance, 2010).

This thesis initially takes focus on a total of four factors.

Two factors are adopted from the already validated research of Herath & Rao (2009b). Two additional factors where less research on the relationship of these factors to policy compliance can be found in current literature are recognized, being:

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

More on these factors, their current level of research and the addition to the model is found in 7.2.1 and 7.2.2.

Although these factors are recognized in relation to compliance to ISP, no relevant research has been found where Information Security Governance or Sense of Ownership are researched as a motivation factor on compliance to ISP.

> *The problem is in the current lack of insight on the effects of promoting the extrinsic motivational factor "information security governance" and the intrinsic motivational factor "sense of ownership" in relation to their influence on the intention of end-users to comply with their applicable ISP in order to protect the organization's information they exchange in the digital domain.*

In order to research the focus areas of this thesis, the base model Herath & Rao (2009b) is usable by adding the motivational factors on (extrinsic) information security governance (Spears & Barki, 2010) and (intrinsic) ownership (Avey et al., 2009).

7.2.1 Addition 1; Information Security Governance

On the extrinsic side of the model a factor named 'Information Security Governance' is added to the model wherein three elements are clustered.

Two of these three elements on information security governance are recognized by Spears and Barki (2010) regarding the term accountability. They see two related ways on accountability being 'formally assigned responsibility' and the 'organizational expectation that a person in a particular role will be informed of and follow policy'. Therefore new roles were introduced being 'data custodian' and 'data steward'. These roles are clearly extrinsic formalized by the organization and their existence is recognized as motivational elements on information security governance and are therefore added to the conceptual model. There is also support from the DAMA DMBOK framework (2008), the ISO 27000-series (NEN-ISO-27001, 2013; NEN-ISO-27002, 2013) and other frameworks on Information Security Governance which describe the same roles and elements.

The ‘learning from the successful information security experiences of others’ is based on the concept of utilizing international best practices for information security (Von Solms & Von Solms, 2004) leading to the use of NEN-ISO 27002:2013 Code of practice for information security controls which includes controls on information classification. The objective of these controls is “to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.” (NEN-ISO, 2013). Information Classification schemes which are extrinsically formalized from an organization perspective as well and their existence is seen as a motivational element on information security governance (Johnston & Hale, 2009). This element is also added to information security governance factor of the conceptual model.

The three added, recognized extrinsic motivational elements for Information Security Governance summed:

1) 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))
2) 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))
3) 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 & Hale, 2009; Puhakainen & Siponen, 2010))

These three motivational elements are all in the area of information security governance and are therefore clustered as motivational factor ‘Information Security Governance’ in the expanded model for this thesis.

7.2.2 Addition 2; Sense of Ownership

On the intrinsic side of the model a cluster named ‘Sense of Ownership’ is added to the model wherein two motivational elements are clustered. The first element 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, & 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. The second element in the factor 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 & Rao, 2009a).

More on sense of ownership is found in the research of Van Dyne & Pierce (2004) on the importance of ‘feelings of ownership’ for the organization, even when employees are not 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 & Allen, 1991). Research showed the linkage between organizational commitment and information security (Olckers, 2013; Stanton, Stam, Guzman, & Caledra, 2003). With the addition of sense of ownership to the model this linkage and its components are researched in the context of compliance to ISP.

8 Subject Matter Experts "Judge/Refine" (Step 1b)

On the 29th of May and the 2nd of June 2015, subject matter expert sessions took place. Such sessions have the goal to judge the theoretical framework of the thesis in preparation of conducting the research. Three subject matter experts (SME) joined the sessions, each with a specific expertise or focus:

- Expert 1: Senior Security Consultant (BSc.) in the role of Corporate Information Security Officer (CISO) with a technical focus. 10+ years of experience in the field of information security.
- Expert 2: Security Consultant (BSc.) in the role of Business Consultant with a focus on process and governance.
- Expert 3: Customer Services Support Professional (MSc.) holding a degree in cognitive psychology with a focus on the end-users intentions part of this thesis.

8.1 Session outcomes

Using a slideshow as a guideline, a structured walkthrough of the theoretical framework took place, starting with the context map (Figure 4) explaining the background of the thesis. Furthermore the experts reviewed the research questions, design & method and the literature to evaluate the conceptual theoretical framework.

Main conclusion of all experts is a high level of rigor in the theoretical framework. The next paragraphs demonstrate the discussions and survey question reviews during the SME sessions.

8.1.1 Discussions

During the first session a discussion took place about the term 'awareness' and the fact that this term is not recognized in the framework as such. The experts agree on the fact that 'awareness' is in the elements of fear (paragraph 6.3.2) and deterrence (paragraph 6.3.1) and they also conclude that 'awareness' is an - so called - 'umbrella term' and cannot as such be described as a separate factor in the framework. To prevent contradictory findings the term 'awareness' will not be included in the framework as a separate factor.

As explained in paragraph 7.1 the role of penalties remained unclear in previous research. A discussion took place whether or not a positive hypothesis on penalties could be stated as part of this research. Such positive approach would turn 'penalties' into 'rewards' as a motivational factor. Elaborating on the 'rewards' term brings in cohesion/synergy to other factors, for example there is cohesion to the 'information security governance' factors found by the experts where different roles could be rewarded for good behavior. Also synergy is discussed to factor 'ownership' where rewarding is only possible to the 'owner' of the information, which isn't always a one-on-one relationship because other roles handle the information as well and therefore it might not be applicable to reward these roles. Bottomline of the discussion is that research on this factor (in negative sense: Penalties, in positive sense: Rewards) should be self-contained because of the contradictory findings in previous research. Goal would be to get more insights on this specific factor before embedding these elements in a multi-factor model.

Especially expert nr. 3 is, because of his background, interested in the framework on promoting end-users behaviors as explained in paragraph 2.3 (in a nutshell: shape conditions - likely to promote motivational factors - influencing the individual's intentions - to perform desired behavior). From his expertise he confirms the framework and explains how influence works by making an extreme example: By taking us back to times of slavery he explains how desired behavior can be reached as well by directly influencing individual's intentions. The modern version used in this thesis and today's organizations is less forced and leaves more space for interpretation by the individual, but in fact works exactly the same. This brings us to the discussion on how to make sure individuals perform desired behavior which learned us that such isn't possible within an organizational context today. The trick is indeed to shape

conditions in such a way they positively affect individuals behavior. This discussion confirmed the applied framework for the thesis.

Accountability is mentioned as a discussion topic by one of the experts: Isn't accountability a separate element or is it covered within the elements of information security governance? The experts agree on the fact that this is covered within information security governance. Details can be found in paragraph 7.2.1 explaining 'formally *assigned* responsibility' and the 'organizational *expectation* that a person in a particular role will be informed of and follow policy' (Spears & Barki, 2010). Also, in paragraph 29.3 a link on accountability to familiarity is reported as an additional finding from the research conducted.

The expectations on the element Sense of ownership and especially of the territoriality items are high during the discussion in the SME session. During the session we discussed the frameworks of Olckers (2013) and Avey et al. (2009) in relation to the several protection motivation theories (e.g. (Herath & Rao, 2009a; Ifinedo, 2012; Johnston et al., 2015; Vance et al., 2012)). Territoriality is related to expressions like: 'this is MINE!'. From there, another car example was mentioned by one of the experts: In this example, in the sense of territoriality to a car one would not allow people to smoke in a car, because 'it's MINE' and they want to protect it. Experts agree on positioning territoriality as prominent as such in the framework as explained in Figure 15, which leads to the last two questions shown in Table 6. Also, in paragraph 29.2 a delta on this aspect is reported as an additional finding from the research conducted.

8.1.2 Survey review

Also the draft version of the survey has been tested during the sessions from which some minor adjustments have been made on survey questions. At the same time this also counts as testing the online survey tooling and the export possibilities of the tooling.

The adjustments are reported in detail in chapter 10, where especially during the SME sessions two items are discussed:

- In the concept version of the survey questions, there are several questions ending with: "…if I comply to policy". The experts mention that each question is related to the dependent variable 'policy compliance intentions' and therefore this should not be an explicit part of the questions as well. These parts are therefore removed from the affected survey questions.
- The same issue is on two of the 'ownership' questions. These questions end with: "… therefore I'm *inclined* to comply to policy". There is an additional issue with such questions, besides the explicit relation to the dependent variable, because they include a conclusion as well. A survey question in general should not include a conclusion to prevent it from measuring other or even multiple constructs than they intent to measure.

As can be seen from above reporting's, the subject matter experts made a valuable contribution to the thesis.

9 Proposed Conceptual model of thesis (Output 1)

The proposed conceptual model for this thesis is presented in Figure 10 below:

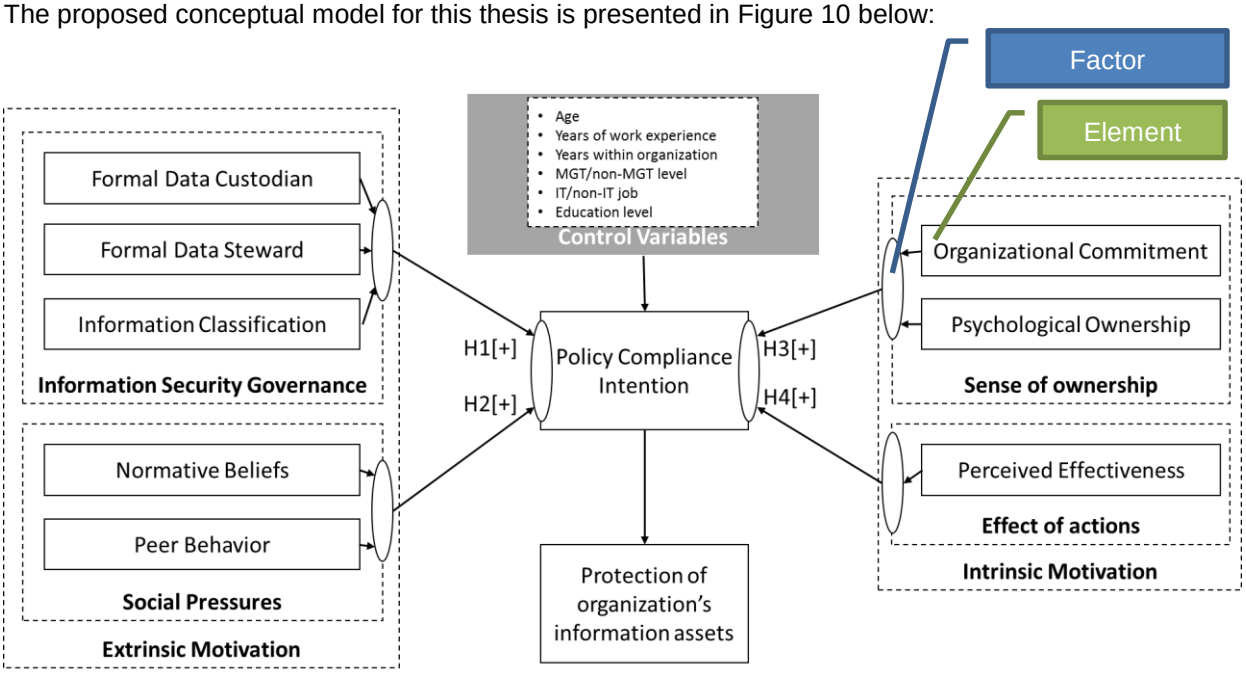


Figure 10 Proposed conceptual model (expanded)

The model in Figure 10 contains one dependent variable (Policy Compliance Intention), being influence by four motivational factors containing a total of 8 elements forming the independent variables. To control whether other variables have an influence on PCI, some control variables are in the model as well. The proposed conceptual model shows the relationships to be researched within the specific context of a given organization.

Hypothesis for model: It is expected to find positive influences on all hypothesized relationships (H1 till H4) in Figure 10 meaning that:

- a formally expressed information security governance (H1) and the insight that governance brings helps the end-users intention to comply to the ISP
- social pressures (H2) helps the end-users intention to comply to the ISP
- it is expected to find that a higher level on sense of ownership (H3) of corporate information assets makes end-users take better care of information and in order to protect they intent to comply more to the policy than in cases of a more abstract level of ownership
- seeing the effects of their actions (H4) also helps the end-users intention to comply to the ISP.

Summarized:

H1(positive)	=	Information Security Governance positively influences PCI
H2(positive)	=	Social Pressures positively influences PCI
H3(positive)	=	Sense of ownership positively influences PCI
H4(positive)	=	Effect of actions positively influences PCI

Some control variables will be included in the conceptual model to test whether these demographics affect the dependent variable (Siponen & Vance, 2010). It is expected that some of the control variables will have a significant effect on the variance of "Policy Compliance Intention" and some conclusion might be drawn from that (D'Arcy et al., 2009). After the pilot survey the control variables will be definitively determined. Up front the control variables Age, Years of work experience, Years and level within organization, IT/non-IT job and Education level are expected to be of influence.

10 Survey design (Step 2a)

Within the scope of answering sub-question 2, the survey tooling is selected and questions are designed into a research instrument (online survey). Also the analysis methods are pre-determined. To test the research instrument, a pilot survey is conducted within a pilot context after which the results are analyzed in order to refine the research instrument where applicable.

The steps are outlined in Figure 11.

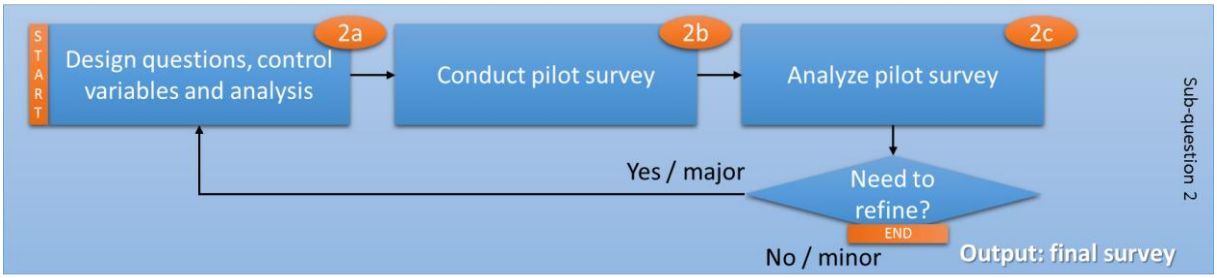


Figure 11 Steps in sub-question 2

10.1 General survey design and tooling

The survey consists of at least two questions per relationship in the conceptual model shown in Figure 10, where each question involves a Likert (Likert, 1932) type scale to indicate a respondent's level of agreement with the statement regarding the likelihood of complying with the information security policies in their organizations (Herath & Rao, 2009a, 2009b).

"Before deciding on the optimal number of response categories for a rating scale, researchers and practitioners may therefore need to perform a trade-off, in the light of the prevailing circumstances, between reliability, validity, discriminating power, and respondent preferences." (Preston & Colman, 2000). From the findings of Leung (2011) is learned that having more scale points seems to reduce skewness, but "There is no major difference in internal structure in terms of means, standard deviations, item—item correlations, item—total correlations, Cronbach's alpha, or factor loadings." (Leung, 2011). Therefore each scale consists of 5 points rating from Strongly disagree, Disagree, Neutral, Agree to Strongly agree.

Electronic survey tooling is applied using a Student License on 'www.enquetesmaken.com'. This tooling satisfies all functional and non-functional requirements for this thesis research. For example it provides all needed possibilities on question design and provides possibilities to apply multiple languages within one integrated survey which is a requirement for the global context. It also fulfils the needs around export possibilities in CSV format providing import possibilities in statistical analysis tooling.

All questions in the survey are mandatory to be answered by the participant. Only completed survey responses are applied in the research.

10.2 Literature mapping

With the conceptual model as a starting point, all factors have a mapping to their main source(s) of literature, as shown in Figure 12.

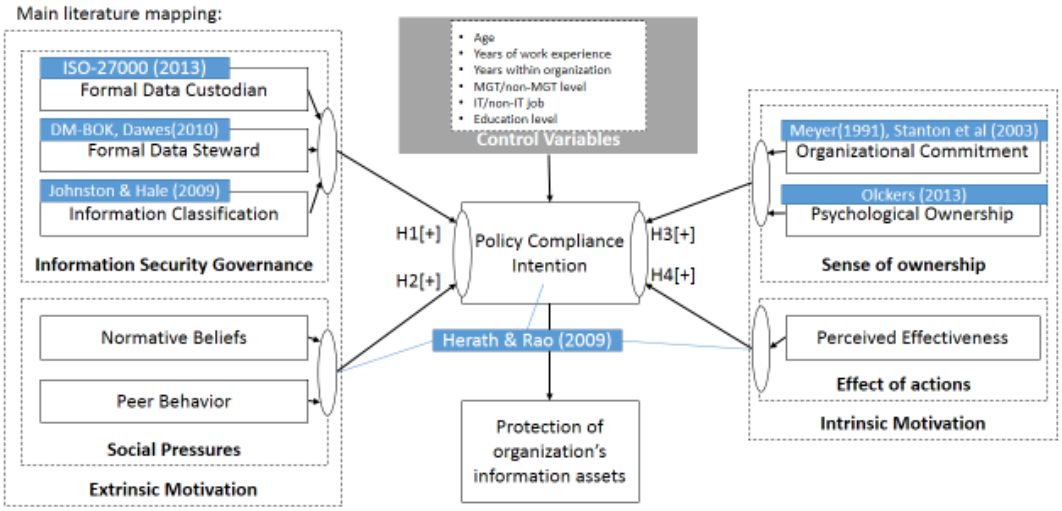
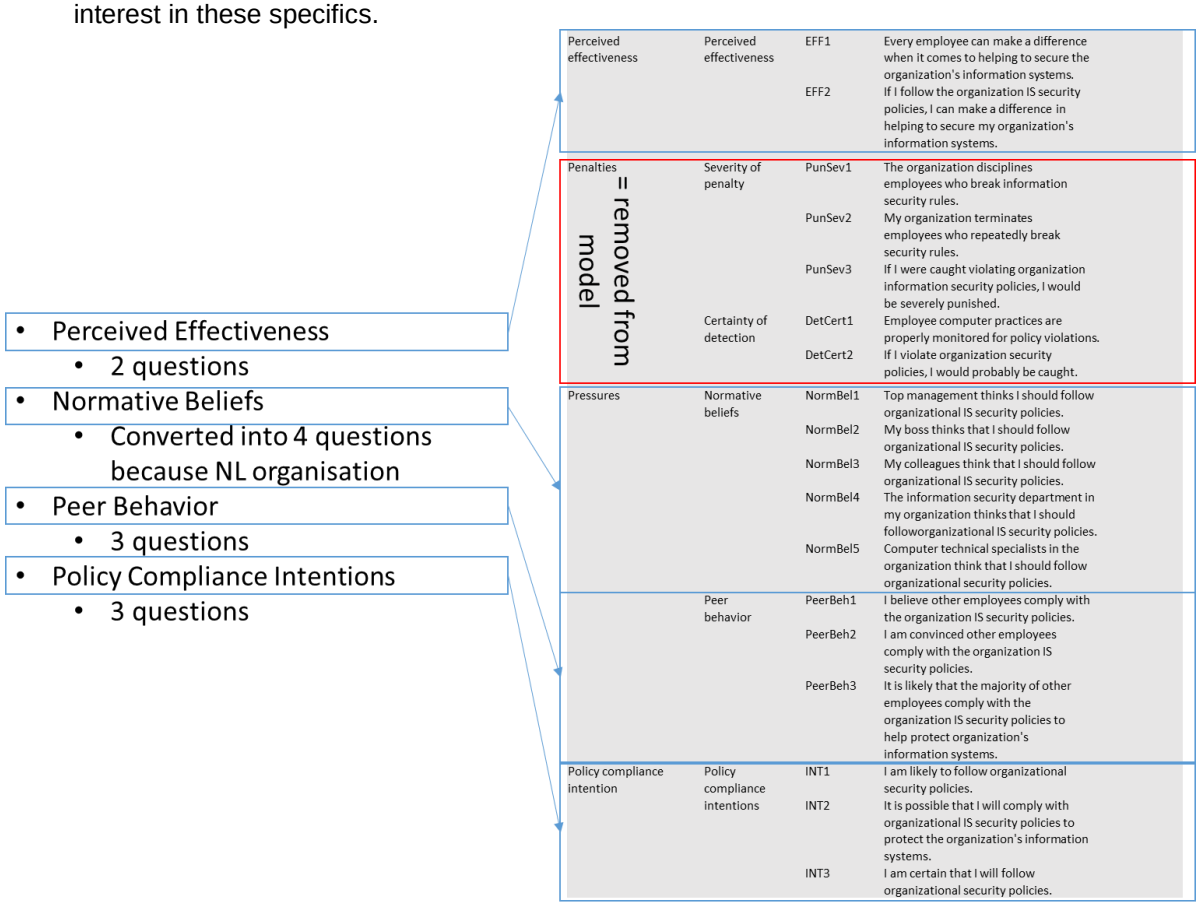


Figure 12 Main literature mapping

Each factor has at least two underlying sources of literature as described in chapter 6.
The base for the conceptual model is found in Herath & Rao (2009b) for which the questions are literally translated or converted from the already validated part of the model as shown in Figure 13. The term 'converted' implies minor textual/grammatical changes in order to align translation between the non-global version (in Dutch) and the global version (in English). These conversions have been additionally reviewed by subject matter expert 3 because of his special interest in these specifics.



Perceived effectiveness	Perceived effectiveness	EFF1	Every employee can make a difference when it comes to helping to secure the organization's information systems.
		EFF2	If I follow the organization IS security policies, I can make a difference in helping to secure my organization's information systems.
Penalties	Severity of penalty	PunSev1	The organization disciplines employees who break information security rules.
		PunSev2	My organization terminates employees who repeatedly break security rules.
		PunSev3	If I were caught violating organization information security policies, I would be severely punished.
	Certainty of detection	DetCert1	Employee computer practices are properly monitored for policy violations.
		DetCert2	If I violate organization security policies, I would probably be caught.
Pressures	Normative beliefs	NormBel1	Top management thinks I should follow organizational IS security policies.
		NormBel2	My boss thinks that I should follow organizational IS security policies.
		NormBel3	My colleagues think that I should follow organizational IS security policies.
		NormBel4	The information security department in my organization thinks that I should followorganizational IS security policies.
		NormBel5	Computer technical specialists in the organization think that I should follow organizational security policies.
	Peer behavior	PeerBeh1	I believe other employees comply with the organization IS security policies.
		PeerBeh2	I am convinced other employees comply with the organization IS security policies.
		PeerBeh3	It is likely that the majority of other employees comply with the organization IS security policies to help protect organization's information systems.
Policy compliance intention	Policy compliance intentions	INT1	I am likely to follow organizational security policies.
		INT2	It is possible that I will comply with organizational IS security policies to protect the organization's information systems.
		INT3	I am certain that I will follow organizational security policies.

Figure 13 Herath & Rao (2009) question conversion

The conversion of questions leads to the following items. The questions are shown in Table 3, Table 4 and Table 5:

Question	Variable
I am likely to follow organizational security policies	PCI1
It is possible that I will comply with organizational information security policies to protect the organization's information systems	PCI2
I am certain that I will follow organizational security policies	PCI3

Table 3 Survey questions on PCI

Question	Variable
Each employee can make a difference in the security of the information systems of my organization	EFF1
I can make a difference in the security of the information systems of my organization	EFF2

Table 4 Survey questions on Effect of actions

Question	Variable
My board thinks I should follow the information security policies of the organization	NORM1
My immediate supervisor thinks that I should follow the information security policies of the organization	NORM2
My colleagues think that I should follow the information security policies of the organization	NORM3
The I(C)T department thinks I should follow the information security policies of the organization	NORM4
It is obvious that the majority of employees comply with the organization information systems security policies to help protect organization's information systems	PEER1
I believe other employees comply with the organization information systems security policies	PEER2
I am sure that other employees comply with the organization information systems security policies	PEER3

Table 5 Survey questions on Social Pressures

For the elements in the factors Sense of ownership and Information Security Governance questions are formulated or converted from the literature shown in the main literature mapping (Figure 12) and additional literature as described using the below steps.

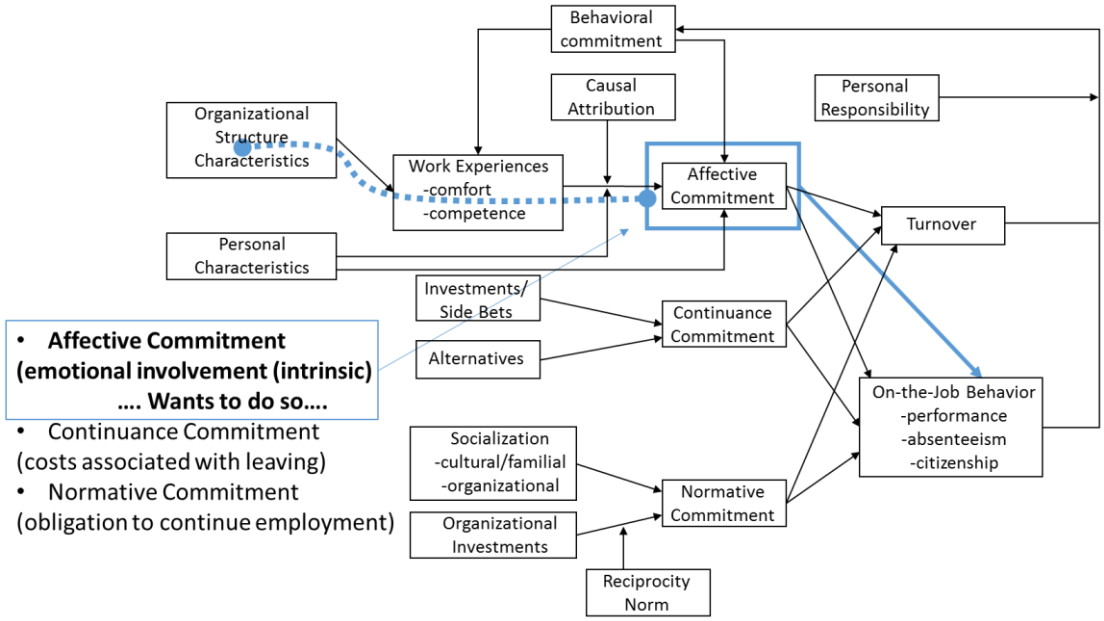


Figure 14 Meyer & Allen (1991) on Affective Commitment

From the research of Meyer & Allen (1991) and Van Dyne & Pierce (2004) is learned that affective commitment is related to psychological ownership. Figure 14 shows the model of Meyer & Allen (1991) and the relationship found in their research from structure – work experiences (Comfort & Competence) to affective commitment leading to 'On-the-Job Behavior'. The questions on 'Organizational Commitment' in the survey are based on both Comfort and Competence as shown in Table 6. Affective commitment is positively related to psychological ownership as well (Avey et al., 2009).

More on psychological ownership is found in Olckers (2013), who developed an instrument to measure psychological ownership. "Psychological ownership emerged recently as a positive psychological resource that could be measured and developed and that could affect the performance of organisations." (Olckers, 2013). Pierce et al. (2003) define psychological ownership as a cognitive-affective construct that is based on individuals' feelings of possessiveness and of being psychologically tied or attached to objects that are material and immaterial in nature.

From the theoretical dimensions described by Olckers (2013), two dimensions are of interest on the intrinsic side of the thesis model on the element of Psychological Ownership as part of the factor Sense of ownership. The other two dimensions described by Olckers (2013) are extrinsic in nature and are taken into account on the extrinsic side of the thesis model. From the dimensions Self-identity and Territoriality, questions are formulated as shown in Figure 15.

The survey questions measuring the elements within the Sense of ownership factor are shown in Table 6.

TABLE 5: Rotated pattern matrix for the four-factor model.

Dimension	Item	Factor 1	2	3	4
Identity					
Item 52	I feel I have a strong bond with the organisation.	**0.919**	-0.011	-0.071	-0.011
Item 43	I feel that this organisation is part of me.	**0.837**	-0.033	0.047	-0.019
Item 51	I personally experience the successes and failures of the organisation as my successes and failures.	**0.752**	-0.039	-0.136	0.035
Item 31	I feel that I belong in this organisation.	**0.742**	0.009	0.175	-0.066
Item 56	I feel that I have common interests with my organisation that are stronger than our differences.	**0.714**	0.056	0.060	-0.157
Item 24	I feel a strong linkage between me and my organisation.	**0.704**	-0.058	0.190	-0.055
Item 34	I feel 'at home' in this organisation.	**0.703**	0.018	-0.201	-0.161
Item 66	I feel that my personal values and those of the organisation are aligned.	**0.693**	0.006	0.168	-0.013
Item 27	I feel as if this organisation is 'MY' organisation.	**0.642**	-0.043	0.052	0.027
Item 40	I feel totally comfortable being in the organisation.	**0.624**	0.098	0.181	-0.078
Item 55	I feel secure in this organisation.	**0.613**	0.003	0.231	0.003
Item 12	I am proud to say that 'this is my organisation' to people that I meet.	**0.586**	-0.020	0.127	-0.023
Item 49	I feel I have a considerable emotional investment in my organisation.	**0.551**	0.056	0.036	0.053
Item 6	I feel the need to defend my organisation to outsiders when it is criticised.	**0.547**	-0.028	0.086	0.086
Item 61	I feel the need to be seen as a member of the organisation.	**0.539**	0.159	0.154	0.154
Item 9	I feel the need to support my organisation's goals and policies.	**0.456**	0.150	0.002	0.002
Responsibility					
Item 47	I accept full responsibility for my actions within the organisation.	0.037	**0.795**	0.004	0.081
Item 54	I accept ownership for the results of my decisions and actions.	0.071	**0.745**	-0.043	-0.046
Item 63	I feel personally responsible for the work I do in my organisation.	0.069	**0.706**	-0.071	0.002
Item 48	I feel I should take the consequences of my work in the organisation.	0.025	**0.678**	0.070	0.064
Item 62	If I cannot deliver on a task for whatever reason, I maintain the responsibility to find an alternative resource or solution.	0.017	**0.653**	0.008	0.008
Item 16	I accept the consequences of my decisions in the organisation.	-0.057	**0.632**	0.096	-0.006
Item 59	If the buck stops with me, I ensure that the task/complaint is resolved successfully every time.	-0.032	**0.630**	-0.057	-0.081
Item 28	I take responsibility for my decisions in the organisation.	-0.051	**0.558**	0.125	-0.019
Autonomy					
Item 23	I take responsibility for my decisions in the organisation.	-0.028	-0.018	**0.775**	0.040
Item 42	I have considerable opportunity for independence and freedom in how I do my work.	0.093	0.064	**0.725**	0.038
Item 29	I am allowed to use my personal initiative and judgement in carrying out my work.	0.108	0.008	**0.705**	-0.036
Item 19	I have the opportunity for independent thought and action.	0.014	0.113	**0.689**	-0.079
Item 38	I have almost complete responsibility for deciding how and when the work is done.	0.217	-0.012	**0.616**	0.113
Item 11	I have the freedom to schedule my work and determine how it is done.	0.074	0.065	**0.598**	0.074
Territoriality					
Item 39	I feel the need to discourage others to invade my work space.	-0.063	0.028	0.032	**0.792**
Item 26	I feel that people I work with should not invade my work environment.	-0.125	-0.009	0.104	**0.700**
Item 35	I feel the need to protect my intellectual property from being used by others in the organisation.	0.035	0.021	0.014	**0.678**
Item 22	I feel the need to protect my belongings from others in the organisation.	0.031	-0.004	0.045	**0.584**
Item 29	I feel I need to defend my work environment from others in the organisation.	0.077	-0.052	-0.081	**0.470**

Extraction method: Maximum likelihood.
Rotation method: Oblimin with Kaiser Normalisation.

Figure 15 Olckers (2003) on Organizational Commitment

Question	Variable
I feel I have a strong bond with the organization	OWN1
I feel comfortable within the organization	COMMIT1
I possess the competences to perform my job well, therefore I'm committed to comply to policy	COMMIT2
I feel the need to protect my information from use by others in the organization	TERR1
I feel the need to protect my organization's information for use by other organizations	TERR2

Table 6 Survey questions on Sense of ownership

The last part of the survey consists of questions measuring the elements within factor Information Security Governance as explained in chapter 6.3.7.

1) The existence of a formally expressed 'Data Custodian'
2) The existence of a formally expressed 'Data Steward'
3) The existence of formally expressed regulation on 'Information Classification' and the consequences of applying classification

These three elements are all in the area of information security governance and are therefore within motivational factor 'Information Security Governance'. The elements 'Data Custodian' and 'Data Steward' have, depending on the organization, a broad responsibility. Besides the security aspects measured within the instrument, these roles might include more aspects on data governance as well (Lee & Strong, 2003). These elements lead to the survey questions listed in Table 7.

Question	Variable
The formalized existence of a functional role 'Data Custodian' helps me to protect my organization's information	CUSTO1
I think a distinction between the owner and the 'Custodian' of information is important	CUSTO2
The existence of a functional role such as a 'Data Steward' helps me to protect my organization's information	STEW1
I think a distinction between the owner and the 'Steward' of information is important	STEW2
The existence of a classification system for information (e.g. public, classified, secret) helps me to protect information	CLASS1
I think it should be clear what kind of information falls in a certain classification level and what consequences apply to assigning a particular classification	CLASS2

Table 7 Survey questions on Information Security Governance

10.2.1 Control variables

To control for explanation of results due to other factors, several control variables were added. These include demographic characteristics of the individual respondent. Age, years of work experience, years within organization, the 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 is of any influence on intentions, the respondents are also asked whether or not they are within the ICT department.

On the numerical questions of age, years of work experience and years within organization the respondents are asked to answer in pre-determined steps/categories. There is a balance chosen in the size of the steps for granularity on the one side and making it possible to conduct an anonymous survey on the other side.

The survey questions on the control variables are shown in Table 8.

Question	Variable
What is your age? - *Dropdown box <25 until >65 in steps of 5 years*	AGE
How many years of experience do you have? - *Dropdown box <5 until >40 in steps of 5 years*	YEARSEXP
How many years do you work within your current organization? - *Dropdown box <1 until >40 in steps of 3 years*	YEARSORG
What is your organizational level where you are currently positioned in? *Dropdown box with values:* - *Operational level* - *Middle management / leadership role* - *Senior management / board level*	LEVELORG
What is the highest degree or level of education you have completed? *Dropdown box with values:* - *Primary education* - *Trade/technical/vocational training* - *Secondary trade/technical/vocational training* - *Higher general secondary education or Highschool* - *Bachelor's degree* - *Master's degree, professional or doctorate degree*	EDUCATION
Do you work within the IT department? (Yes / No)	ICT

Table 8 Survey questions on control variables

10.2.2 Information Security Policy status

To get more feeling on the context and status of the policy, several questions are included measuring status and perception around ISP.

From the idea that an end-user should be familiar with ISP before being able to comply (Ifinedo, 2014; NEN-ISO-27002, 2013) one question is added. From the idea that it helps to comply once an end-user can associate itself with ISP (Albrechtsen, 2007; Posthumus & Von Solms, 2004) another question is added. To get insights on the 'conflict of interest' discussion from paragraph 2.5 (Ifinedo, 2012; Siponen & Vance, 2010) one question is added.

The survey questions on the insights of ISP variables are shown in Table 9.

Question	Variable
I am familiar with the current information security policy of my organization	ISP1
The resources provided by my organization in order to carry out my work, allow me to perform my duties in accordance with the policy.	ISP2
It takes so much time to perform my work duties in accordance with the information security policy that I can't get my job done.	ISP3

Table 9 Survey questions on ISP status

10.3 Variable overview

A total mapping of the variables measured in the survey is shown in Figure 16.

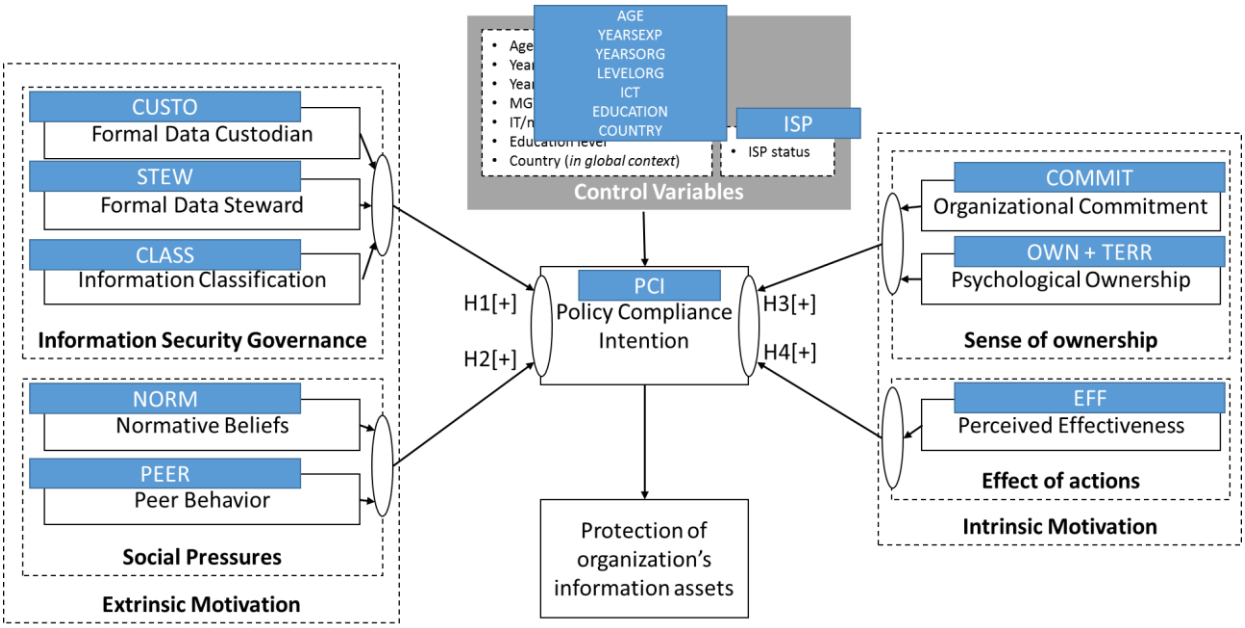


Figure 16 Mapping of variables (overview)

10.3.1 Constraints & limitations

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. This concern needs to be minimized by informing the participants that the submission of truthful responses would never yield negative consequences.

In the introduction statements of the survey the following is mentioned:
"The survey outcomes are anonymous and will be processed anonymously. Please answer truthfully, even when your answers are not desirable to your organization."

Specific assumptions and context are applicable to the research:

- Research is focused on the positive influence of end-users working on organizational information systems.
- ISP is present (whether informal of formal) and, in case of formal ISP, communicated to end-users.
- Users have a benign approach, there is no evil sense.

11 Pilot Survey + Analysis (Step 2b and 2c)

In order to refine the research instrument created in Step 2a, a pilot survey is conducted and analyzed within a pilot context.

11.1 Research context 1: Company in ICT Security Sourcing

The research context used for the pilot survey is a Dutch company in the business of ICT Security (namely my employer, Motiv IT Masters B.V.). Started in the year 1998 as a sparring partner, system integrator and problem solver for its customers searching for innovative ICT security solutions.

Motiv currently consists of 100+ employees and contractors and is mainly engaged in the BeNeLux area. More details on demographics of this context can be found in Appendix B (Demographics of research context 1) on page 91.

For this context information security and ISP is very relevant, because all core activities have to do with information security.

11.2 Conducting the pilot survey (Step 2b)

On the 2nd of June all employees and contractors of Motiv, as end-users of the corporate information systems were requested to fulfill the pilot survey before the 10th of June. A reminder was sent on the 4th of June. A total of 57 persons responded in full leading to a 57% response rate as shown in Table 10.

	Context 1 (Pilot)
Requests	100
Responses (full)	57
Response rate	57,00%

Table 10 Response rate on pilot survey

12 Statistical analysis (basic steps)

Statistical Package for the Social Sciences (SPSS) software is used to analyze the conducted 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).
    - ✓ Factor analysis will be done to determine the factor loadings in order to analyze the correlations between the items and determine the correct factors. These factors should predict the dependent variable 'Policy Compliance Intention' and are the so called predictor (independent) variables (Bryman & Bell, 2007).
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 (Figure 20), as a group (factor or element(s) of factor) go together.
    - ✓ The most commonly used reliability statistic Cronbach's alpha is used for reliability analysis (Urdan, 2010). The Cronbach's alpha (with a Greek symbol of α) 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 on the ordinal variables of the determined factors and elements using the below steps:
    - ✓ Determine how much the factors (predictor variables) are significantly related to, or predictive of the dependent variable 'Policy Compliance Intention'
    - ✓ The strength of each relationship between each predictor variable and the dependent variable *"while controlling for the other predictor variables in the model"* (Urdan, 2010) meaning it is possible to examine whether a predictor variable is related to the dependent variable after taking out the portion of the variance of another dependent variable that has already been accounted for.
    - ✓ Determine the relative strength of each predictor variable and determine the way each variable contributes as a predictor.

    The process will follow the procedures explained in detail in Urdan (Urdan, 2010, chap. 13). Reason to follow these procedures lies in the fact that *"Multiple regression analysis provides a wealth of information between predictor variables and dependent variables"* (Urdan, 2010, p. 156).

13 Analyze pilot survey (Step 2c)

Following the steps outlined in chapter 12 the pilot survey responses are analyzed. First, data is **imported** and **recoded** and textual variables are turned into numerical values within the data file.

13.1 Factor analysis of context 1 (pilot)

An exploratory factor analysis is conducted on a set of the independent items from the survey. The factor analysis, using principal components extraction and varimax with Kaiser Normalization factor rotation, produced 9 factors with eigenvalues greater than 1.0. Suppressing absolute values below 0,3 gives the result as shown in Table 11.

Rotated Component Matrix[a]

	Component								
	1	2	3	4	5	6	7	8	9
EFF1		,893							
EFF2		,879							
NORM1	,800								
NORM2	,680								
NORM3	,551		,303				-,523	-,317	
NORM4	,796								
PEER1			,813						
PEER2			,863						
PEER3						-,769			
OWN1				,843					
COMMIT1				,856					
COMMIT2		,418	,316	,449	,322				,304
TERR1									,912
TERR2								,826	
CUSTO1						,795			
CUSTO2			-,340			,494			,376
STEW1	,340						,749		
STEW2				,404			,740		
CLASS1					,809				
CLASS2					,833			,305	

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

a. Rotation converged in 9 iterations.

Table 11 Factor analysis of context 1

The effect seen on component 6 (for variable PEER3) is further explained in chapter 13.1.1 note 1.

The effect seen on component 8 and 9 on the measurements on element territoriality is explained by the delta between the need to protect the information from the organization for use by others *in* the organization versus for use *by other* organizations. These variables do not measure a single construct and are therefore seen as separate components in the factor analysis.

13.1.1 Reliability analysis of context 1 (pilot)

The **reliability analysis** on the factors as seen in the factor analysis took place leading to the results shown in Table 13. The values represent the Cronbach's Alpha (α) of the factor / element.

α	***Rule of thumb*** (Gliem & Gliem, 2003)
> .900	**Excellent**
> .800	**Good**
> .700	**Acceptable**
> .600	**Questionable**
> .500	**Poor**
< .500	**Unacceptable**

Table 12 Cronbach's Alpha index

According to the 'Rule of thumb' index show in Table 12, a value above 0,700 is considered 'reliable' (Gliem & Gliem, 2003).

Factor / element	Context 1 (Pilot)	Comment
Policy Compliance Intention INT1 INT2 INT3	α = 0,844	**Reliable**
Normative Beliefs NORM1 NORM2 NORM3 NORM4	α = 0,725	**Reliable**, expected to be even more reliable when the additional question designed from the feedback in step 2b (item 4) is added: NORM5
Effect of actions EFF1 EFF2	α = 0,861	**Reliable**
Peer Behavior PEER1 PEER2 ~~PEER3~~	α = 0,815	**Reliable** without PEER3 variable. See note 1 below table.
Data Governance CUSTO1 CUSTO2 STEW1 STEW2	α = 0,424	**Not yet reliable**, in fact unacceptable, but expected to be reliable when the number of respondents is higher, e.g. N=>100. See note 2 below table.
Information Classification CLASS1 CLASS2	α = 0,662	**Not yet reliable**, but expected to be reliable when additional question designed from the feedback in step 2b (item 6) is added: CLASS3
Sense of Ownership COMMIT1 COMMIT2 OWN1	α = 0,678	**Not yet reliable**, but expected to be reliable when question is re-designed from the feedback in step 2b (item 5).

Table 13 Reliability analyses for context 1

Note 1) Peer Behavior measures the perception on the intentions of the other employees within the organization. PEER1 and PEER2 measure 'I believe' and 'It is obvious' where PEER3 measures 'I am sure'. There is a delta between PEER1/PEER2 and PEER3 which can be declared because PEER3 measures an assumed fact instead of a perception. Therefore this will be handled as different constructs in the analysis of the other non-pilot contexts.

Note 2) Data Governance (including the elements 'Formal Data Custodian' and 'Formal Data Steward') are not measured as reliable, because α < 0,700 (0,424). However, in the factor analysis these elements do form a factor and analyzing correlation coefficients with Policy Compliance Intentions shows significant correlations. This element is expected to become reliable once the number of respondents is above N=>100. Therefore this will be handled as a single construct in the analysis of the other non-pilot contexts.

13.1.2 Regression analysis of context 1 (pilot)

The **regression analysis** testing took place with below limitations in mind:

- Factor analysis and reliability analysis showed some uncertainties on the factors and their reliabilities as reported in 13.1.1.
- The number of respondents is somewhat low (N=57) for a regression analysis with 1 dependent variable and 6 predictor variables but will result in an indication of the path coefficients.

Despite the above limitations a multiple regression analysis is conducted to examine the predictors of the Policy Compliance Intention factor. Six predictors were simultaneously entered into the model:

- Normative Beliefs (element of factor Social Pressures)
- Peer Behavior (element of factor Social Pressures)
- Effect of actions
- Sense of ownership
- Information Classification (element of factor Information Security Governance)
- Data Governance (combination of Custodian and Steward and element of factor Information Security Governance)

Together, these predictors account for 45% (adjusted R2 = 0,450) of the variance in PCI (Policy Compliance Intention). Three of these variables were significant predictors of PCI. Normative Beliefs (β = .619) and Effect of actions (β = .289) were the strongest predictors, followed by Information Classification (β = .183).

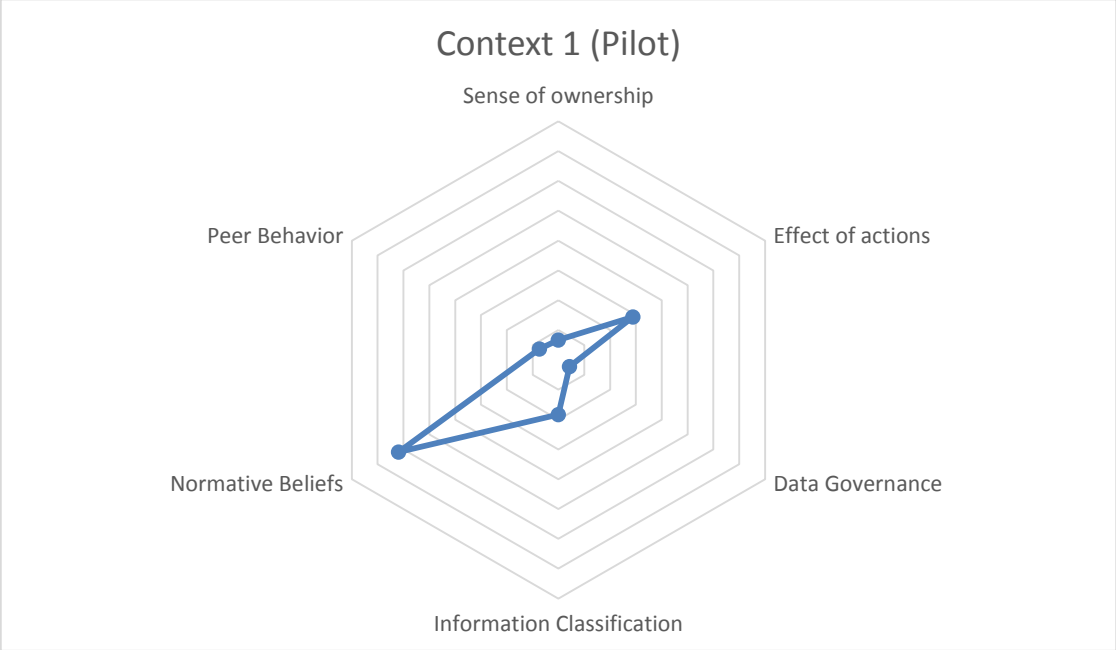


Figure 17 Path coefficients for context 1

Despite the limitations mentioned, the path coefficients shown in Table 14 and Figure 18 give a good indication on the relevance and relations of the motivational factors on PCI for this specific context.

Context 1 (Pilot)	***R2=***	***44,96%***
Sense of ownership	β =	0,067
Effect of actions	β =	0,289
Data Governance	β =	0,044
Information Classification	β =	0,183
Normative Beliefs	β =	0,619
Peer Behavior	β =	0,073

Table 14 Path coefficients for context 1

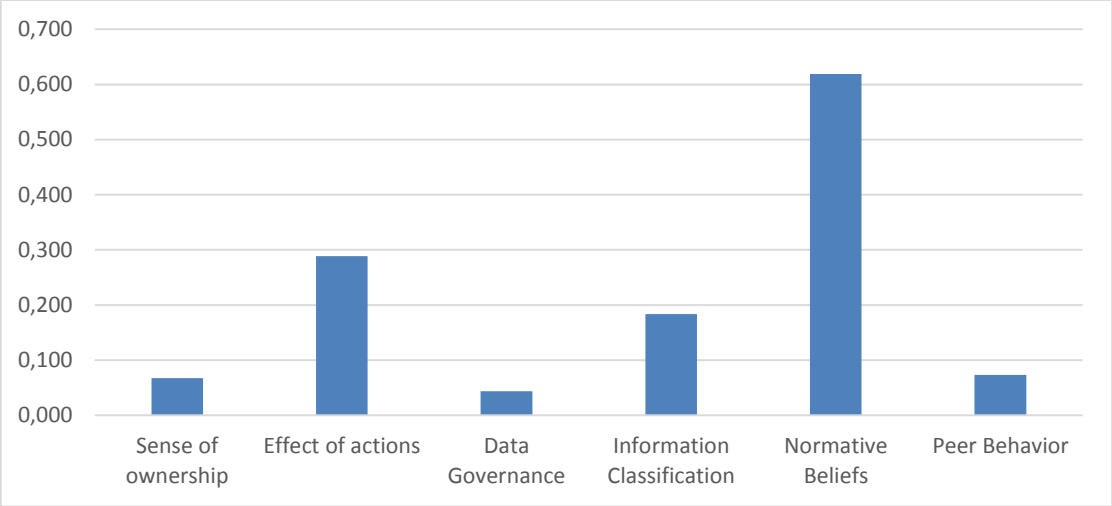


Figure 18 Path coefficients for context 1

The findings reported partly support for the hypothesis on the conceptual model as stated in chapter 9. Positive influences on three of the hypothesized relationships are found in the research findings shown in Table 15:

Nr.	Hypothesis	Result
H1+	Information Security Governance positively influences PCI *(especially the element Information Classification)*	Supported
H2+	Social Pressures positively influences PCI *(especially the element Normative Beliefs)*	Supported
H3+	Sense of ownership positively influences PCI	No support
H4+	Effect of actions positively influences PCI	Supported

Table 15 Results on hypothesis for context 1

13.1.3 Further analysis of context 1(pilot)

The survey also contains several control variables which are included to enhance the insight into ISP compliance for the specific context. For this context the control variables measure Age, Years of experience, Years within current organization, Organizational level currently positioned, the highest degree or level of education completed and whether a person works within the IT department. These variables show no significant coefficient on the dependent variable PCI for this specific context.

During the survey, the participants were asked to indicate whether they agree or disagree with some statements about the information security policy within their organization. The correlation between the question "I am familiar with the current information security policy of my organization" and PCI was positive, moderately strong and statistically significant ($r=.36$, $p < 0.01$).

The correlation between the question "The resources provided by my organization in order to carry out my work, allow me to perform my duties in accordance with the policy" and PCI was positive, moderately strong and statistically significant ($r=.33$, $p < 0.05$).

		PCT	***ISP1***	***ISP2***
PCI	**Correlation Coefficient**	**1,000**	**,361****	**,326***
	Sig. (2-tailed)		**,006**	**,013**
	N	**57**	**57**	**57**

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

Table 16 Correlations on ISP

13.1.4 Revisions on survey instrument

For the pilot survey all participants were also asked to comment on the survey both on content and design. The feedback provided made it possible to improve the pilot survey on 6 items. Items are classified as minor as long as the subsequent revisions do not lead to uncertainties in conducting and analyzing the final survey instrument and research:

Minor 1) One additional question is designed around the opinion of the end-users whether the ISP is applicable to their organization.
Minor 2) A question on the amount of time and effort is split in two separate questions because these two elements should be measured separately.
Minor 3) One additional question is designed around the 'conflict of interest' element: 'getting my job done comes before information security'.
Minor 4) On the survey questions about the Normative Beliefs factor the 'staff officers and advisors' in an organization were not taken into account. Therefore an additional question is designed.
Minor 5) On the Sense of ownership factor one question concluded in 2 variables namely the possession of competences and their linkage to intentions. The last part is removed because intentions are measured separately in the Intentions factor.
Minor 6) On the Information Security Governance factor on element Information Classification one question measured 'clearness' as well as 'consequences' of classification. This question is split into 2 separate questions because these two elements should be measured separately.

The outcomes shown in Table 16 and the feedback on the pilot survey noted as minor 1 till 3 show the relevance/ importance of these statements which leads to additional questions on the status of ISP within an organization making a total of 6 (revised) questions for this part of the final survey.

Question	Variable
I am familiar with the current information security policy of my organization	ISP1
I think the current policy is appropriate for my organization	ISP2
The resources provided by my organization in order to carry out my work, allow me to perform my duties in accordance with the policy.	ISP3
It takes more time to perform my work duties in accordance with the information security policy.	ISP4
It takes more effort to perform my work duties in accordance with the information security policy.	ISP5
Getting my job done comes before information security.	ISP6

Table 17 Survey questions on ISP (revised after pilot)

Minor 4 leads to one additional question on Social Pressures:

Question	Variable
The staff officers and advisors in my organization think that the information security policy should be followed	NORM5

Table 18 Survey questions on Social Pressures (added)

Minor 5 leads to a revised question on Sense of ownership, leaving out the linkage to intentions:

Question	Variable
I possess the competences to perform my job well~~, therefore I'm committed to comply to policy~~	COMMIT2

Table 19 Survey questions on Sense of ownership (revised after pilot)

Minor 6 leads to the split of CLASS2 variable in separate questions:

Question	Variable
I think it should be clear what kind of information falls in a certain classification level	CLASS2
I think the consequences of assigning a particular classification should be clear	CLASS3

Table 20 Survey questions on Information Security Governance (revised after pilot)

Since no major revision took place after the pilot survey, the instrument is validated and can be applied to conduct the final surveys.

14 Final survey instrument (Output 2)

Because of the global intentions of the instrument two integrated versions of the survey are available for final conduct. These can be found in chapter 23.1 for the Non-global version (in Dutch) and chapter 23.2 for the Global version (in English) and are constructed as follows.

The tooling makes it possible for the convenience of the end-users to choose between language on the first screen presented as shown in Figure 19.

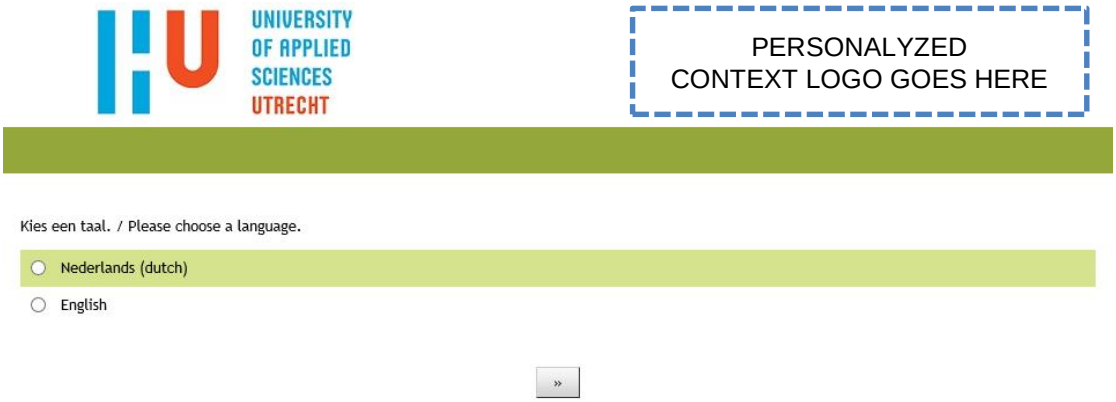


Figure 19 Survey instrument start-up screen

First some introduction texts, instructions and definitions used are presented followed by the demographics information collection. On the second page users are asked to indicate whether they agree or disagree with the statements about the information security policy within their organization. They are asked to choose the answer position they find most applicable to their situation or opinion.

The different parts are presented in below order:

1) The information security policy of your organization
2) What is your expectation on the effectiveness of an information security policy
3) Assess the role of your work environment in relation to compliance with the information security policy
4) Assess your intentions to follow the security policies of your organization
5) Assess the role of ownership in compliance with the information security policy
6) Assess the role of governance in following up the information security policy

Just before the last part a set of definitions is explained:

- '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.

After fulfilling the survey a THANK YOU page is shown.

The final survey can be found in Appendix A (Final survey instrument).

15 Final Conceptual model

The final conceptual model for this thesis is presented in Figure 20 below:

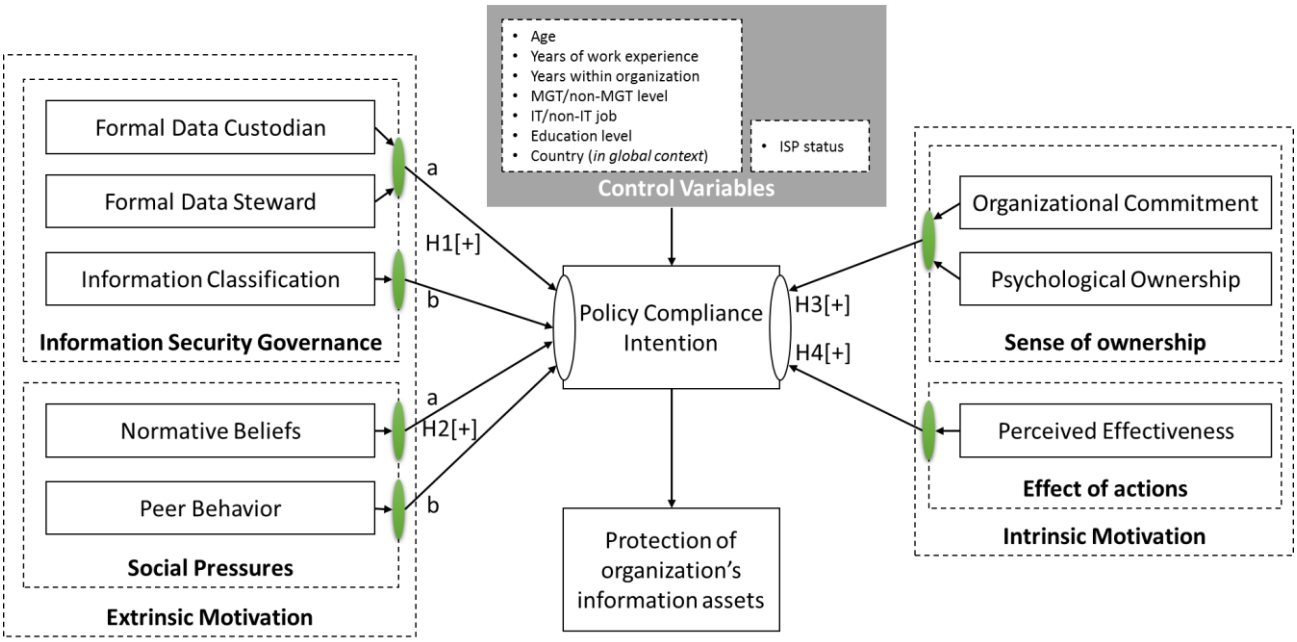


Figure 20 Final model

The model in Figure 20 still contains one dependent variable (Policy Compliance Intention), but in the final model being influenced by six instead of four main factors containing the total of 8 elements forming the independent variables. To control whether other variables have an influence on PCI, some refined control variables are in the model as well.

The model shows the relationships to be researched within the specific context of a given organization.

Hypothesis for model: It is expected to find positive influences on all hypothesized relationships (H1 till H4) in Figure 20:

H1(positive)	Information Security Governance positively influences PCI
a)	by elements of data governance measured separately
b)	by element information classification measured separately
H2(positive)	Social Pressures positively influences PCI
a)	by element of normative beliefs measured separately
b)	by element of peer behavior measured separately
H3(positive)	Sense of ownership positively influences PCI
H4(positive)	Effect of actions positively influences PCI

The control variables Age, Years of work experience, Years and level within organization, IT/non-IT job and Education level are in the final model. For global contexts also the country where the respondent resides is added as a variable. ISP status is added in the final model to get more feeling on the status of the policy and the context.

16 Conduct Final Surveys (Step 3)

Within the scope of answering sub-question 3, the final research instrument is applied to organization contexts. The steps are outlined in Figure 21.

Figure 21 Steps in sub-question 3

For conducting the final surveys a total of 25 organizations were selected during the proposal phase of this thesis. Goal was to have at least one, preferably two research contexts available. During the thesis phase all organizations were consulted for participation in the research where in the end four organizations responded in an enthusiastic manner and were able to get the needed mandate for sending out the distribution email for participation in the survey.

Main reason for most organizations to not participate in the survey is the timing of the research. A common argument is they currently do not have the capabilities to follow up on the research in an appropriate way. This lack of capabilities/capacity to follow up makes the organizations reluctant to participate in the research at the moment. Asking the end-users to spend their time on some critical questions on ISP without proper following up on their responses, might turn the end-users down and possibly an opposite effect is reached.

The contexts that finally participated in the research are described in the following chapters.

Context 1 (conducted in pilot): Company in the business of ICT Security (described before)
Context 2: Healthcare Consultancy and Insurance company
Context 3: Marketing Technology company (Global context)
Context 4: Retail company
Context 5: Financial Services company

16.1 Context 2: Healthcare Consultancy and Insurance

Research context 2 is found at a healthcare consultancy and insurance organization founded over 90 years ago. The organization includes, among others, an insurance unit and thus is subject to supervision by DNB (De Nederlandsche Bank). To this end, DNB operates as an independent central bank and supervisor for this organization.

Focus of the organization is on the Dutch market. All activities together the company employs approximately 700 FTE's (Full Time Equivalent).

The organizational units (departments) collect and process personal data. Therefore information security is an important topic within the organization. In particular for the insurance unit this also includes the collection of medical/health related data as part of their operation.

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.

Furthermore it is notable that the company is very aware of the fact that they should consciously manage the information of its customers! Especially because the company wants to be seen as the trusted advisor by its customers.

A number of end-users spread equally across the organization is selected to conduct the survey as can be seen in Figure 22. The survey request is distributed from the risk management department, part of "Finance, ICT & Risk".

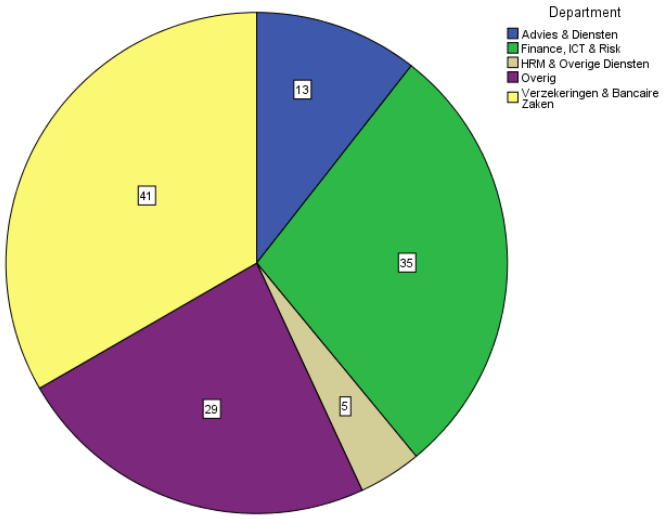


Figure 22 Number of respondents per department of context 2

More details on demographics of this context can be found in Appendix C (Demographics of research context 2) on page 92.

16.2 Context 3: Marketing Technology (Global context)

Research context 3 is found at a marketing technology organization founded in 1992 and through numerous acquisitions and research & development 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.

Furthermore the organizations holds ISO27001:2005 certification and in 2015, transitioning to ISO27001:2013 is planned. Together with the transitioning the organization continues to expand the scope of certification across other products and regions.

All end-users working at the 'DevOps' unit/part of the organization are selected to conduct the survey. These users are spread over several departments as can be seen in Figure 23. The survey request is distributed from the board level using a newsflash.

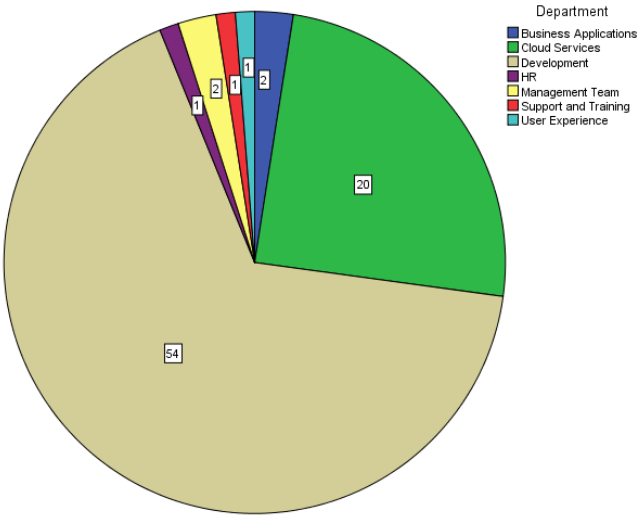


Figure 23 Departments of context 3

As mentioned, context 3 is a global organization and the main language is English. As can be seen in Figure 24 the respondents reside global and even the respondents from the Netherlands sometimes choose the English version of the survey.

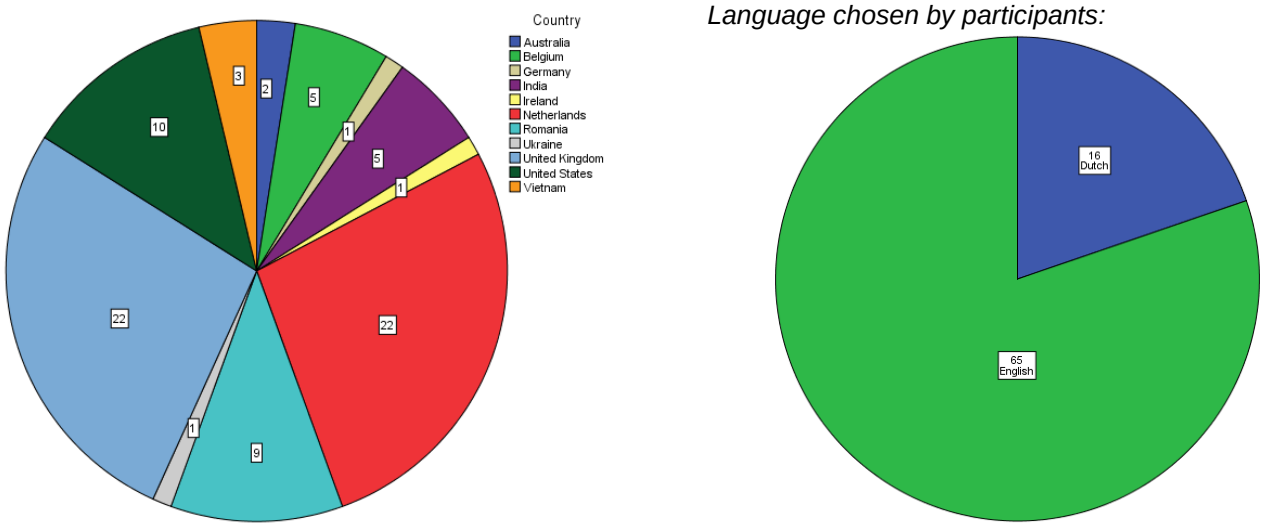


Figure 24 Number of respondents/chosen language of context 3 (global context)

More details on demographics of this context can be found in Appendix D (Demographics of research context 3) on page 93.

16.3 Context 4: Retail

Research context 4 is found at a 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. This retailers focus is on a wide range of products and attractive prices.

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. Also their impressive logistic logics (proprietary and therefore of high value as a competitive differentiator) and combined store/web-shop concept makes IT and security more important than ever.

A number of end-users from the ICT and finance departments are selected to conduct the survey as can be seen in Figure 25. Both departments are positioned in the BeNeLux head office. The survey request is distributed from the board level of the BeNeLux head office.

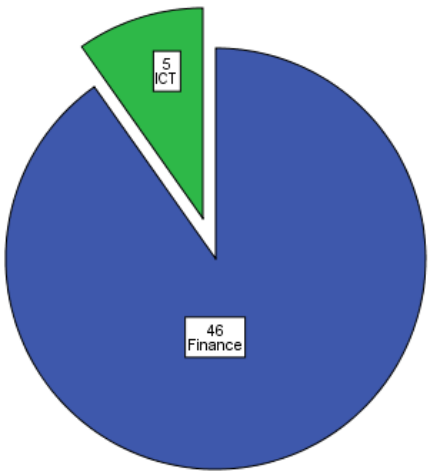


Figure 25 Departments of context 4

More details on demographics of this context can be found in Appendix E (Demographics of research context 4) on page 94.

16.4 Context 5: Financial Services

Research context 5 is found at a financial escrow services organization which operates as an independent third party service provider in the management of mortgages and consumer loans. They operate their services for various national and international financial organizations.

All activities together the company employs approximately 260 FTE's (Full Time Equivalent). Offering these services brings a great responsibility on information security. Therefore the company possesses a high level at Fitch Ratings[1]. Furthermore, since service organizations can communicate information about its controls through a Service Auditor's Report the organization holds an ISAE 3402 type II certification report on their sourcing of financial services. Both the ratings and the certification focus a lot around aspects of 'trust' and therefore information security is very relevant within this context.

The full organization is part of the context. All end-users of information systems are requested to conduct the survey. The number of respondents per department can be found in Figure 26. The survey request is distributed from the board level.

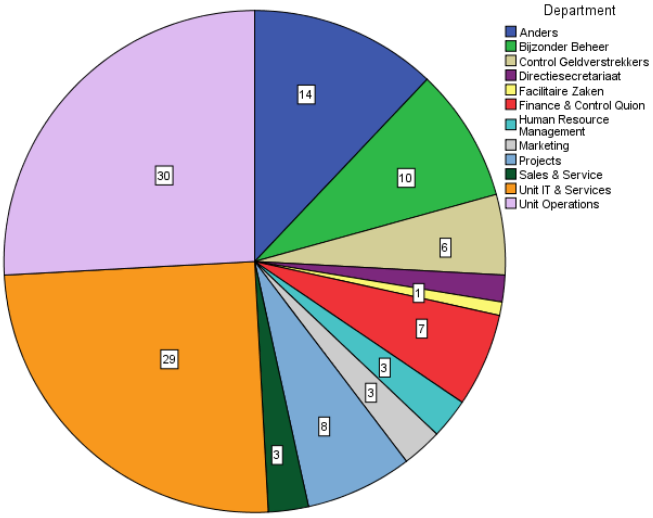


Figure 26 Departments of context 5

More details on demographics of this context can be found in Appendix F (Demographics of research context 5) on page 95.

[1] https://www.fitchratings.com/about

17 Measurements (Output 3)

For each of the four contexts, the survey participation request is distributed by email using a fixed approach and using similar introduction statements. Per context extra effort is made to emphasize the importance of participation for the specific target group within the distribution email.

For example the distribution email for context 3 contained:
"*Currently <organization> maintains an ISO27001 certification for <snip> and soon we hope to expand the scope of this certification to other products. This requires the information security team to create new security policies, procedures and working instructions. While we are preparing the scope expansion and the policies we are willing to measure how familiar you are with the current security policies, the ISMS and your role in data protection. Having this insights helps <organization> to introduce the new ISMS in a more effective way*."

Each context was given the same amount of time to fulfill the survey. Table 21 show the status on the closing date of the last request.

	Context 2	Context 3	Context 4	Context 5	Total-4 contexts
Requested	403	180	110	300	Sum of 993
Started	179	103	72	163	Sum of 517
Responses	123	81	51	116	**Sum of 371**
Response rate	30,52%	45,00%	46,36%	38,67%	**Average: 40,14%**

Table 21 Response rate on final surveys

All context together form a total of 371 fulfilled surveys with an average response rate just above 40%. According to the findings of Baruch & Holtom (2008) this is above average in case of data collection within organizations. A reason the response rate being somewhat lower than personally expected is probably found in the time effort needed to fulfil the survey. This effect can be seen in Table 21 on the number of started responses which is considerably higher compared to the number of fulfilled responses. The reasons for not responding will certainly be diverse in nature.

Two principal reasons for not responding are failure to deliver the questionnaires to the target population (e.g. wrong address, absent from work) and the reluctance of people to respond (Baruch, 1999). As can be learned from the number of respondents started versus the respondents who completed the survey both principal reasons might apply in this case.

Especially in context 2 the response rate is lower with regards to the other contexts. From the informal interview with the Security Manager of context 2 is learned that the organization could be named 'over-surveyed'. Over-surveying means that employees are flooded with questionnaires (Baruch & Holtom, 2008). Together with the problem of being over-surveyed the request email of context 2 is distributed from the middle-management level of the organization instead of the strategic/board level as is the case for the other contexts.

Regardless of the above remarks the results are very satisfactory and provide the needed data to be analysed in the next step of the thesis.

18 Analysis (Step 4a)

Within the scope of answering sub-question 4, the conducted survey results / measurements are statistically analyzed. From these analysis conclusions are drawn and reported giving answer to the research question.

The steps are outlined in Figure 27.

Figure 27 Steps in sub-question 4

All measurements from the four contexts are analyzed using the steps outlined in chapter 12. First, data is **imported** and **recoded** and textual variables are turned into numerical values within the data file 'total-4' which form a dataset to first statistically analyze the final model and research instrument and provide insights in the total of measured contexts using the 371 responses.

After analyzing the final model and research instrument the same dataset is used to make analysis *per context* after which these results are combined and compared to the results seen in the total of four contexts.

18.1 Factor analysis

A factor analyses is conducted on all items measuring the motivation factors and PCI from the survey using the responses of the dataset 'total-4' which include all answers to the survey from context 2 till 5 (all except the pilot context). This factor analysis, using principal components extraction and varimax with Kaiser Normalization factor rotation, produced the expected 7 factors with eigenvalues greater than 1.0. Suppressing absolute values below 0,326 gives the rotated result as shown in Table 22.

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.

Table 22 Factor analysis of total-4

The outcomes of the factor analysis in Table 22 show evidence on the items in the survey belonging together per factor/element and measure a single construct per factor/element.

18.2 Reliability analysis

The **reliability analysis** on the factors as seen in the factor analysis took place leading to the results shown in Table 23. The values represent the Cronbach's Alpha (α) of the factor / element again for the final model using the responses of the dataset 'total-4' which include all answers to the survey from context 2 till 5 (all except the pilot context).

Factor / element	Context total-4	Comment
Policy Compliance Intention INT1 INT2 INT3	α = 0,827	**Reliable**
Normative Beliefs NORM1 NORM2 NORM3 NORM4 NORM5	α = 0,892	**Reliable**
Effect of actions EFF1 EFF2	α = 0,878	**Reliable**
Peer Behavior PEER1 PEER2	α = 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**

Table 23 Reliability analyses for total of 4 contexts

As a reminder the below rule of thumb is applied:

α	***Rule of thumb*** (Gliem & Gliem, 2003)
> .800	**Good**
> .700	**Acceptable**

This reliability analysis was performed to examine the internal consistency of the seven factors produced by the factor analysis in chapter 18.1. This reliability analysis revealed that the items within the factors found do belong together, as can be seen on the α scores reported. The items in Peer Behavior and Data Governance factors produced a scale with an acceptable level of internal consistency (> .700). The other factors all produced a reliable scale of internal consistency (> .800).

18.3 Regression analysis (total-4)

For the 'total-4' dataset a multiple regression analysis is conducted to examine the predictors of the Policy Compliance Intention factor. Six predictors were simultaneously entered into the model:

- Normative Beliefs (element of factor Social Pressures)
- Peer Behavior (element of factor Social Pressures)
- Effect of actions
- Sense of ownership
- Information Classification (element of factor Information Security Governance)
- Data Governance (combination of Custodian and Steward and element of factor Information Security Governance)

From the analysis the model summary shown in Table 24 is formed.

Model Summary

Model	R	R Square	Adjusted R Square
1	,509[a]	,259	,257
2	,610[b]	,372	,369
3	,626[c]	,392	,387
4	,640[d]	,410	,403
5	,646[e]	,417	,409
6	,647[f]	,419	,409

Table 24 Model summary of total-4 regression analysis

Together, as can be seen in the model summary 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. As can be seen in Table 24 the adjusted R2 is equal for model 5 and 6.

From the analysis the path coefficients shown in Table 25 is formed.

	Standardized Coefficients		
	Beta	t	Sig.
(Constant)		14,868	,000
NORMMEAN	,509**	11,351	,000
OWNMEAN	,358**	8,159	,000
CLASSMEAN	,151**	3,408	,001
PEERMEAN	,146**	3,356	,001
EFFMEAN	,092*	2,151	,032
DATAGOVMEAN	,044	,963	,336

***. Significant at the 0.01 level*

**. Significant at the 0.05 level*

Table 25 Coefficients table of total-4 regression analysis

The coefficients table shows 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 and, as expected from the results in the model summary in Table 24. Data Governance (combination of Custodian and Steward and element of factor Information Security Governance) does not show significant paths in the total-4 model.

18.4 Path Analysis

Analysis of the total-4 dataset shows an averaged image of the paths shown in Figure 28. Please keep below 'pattern' in mind while reading the remaining part of this chapter.

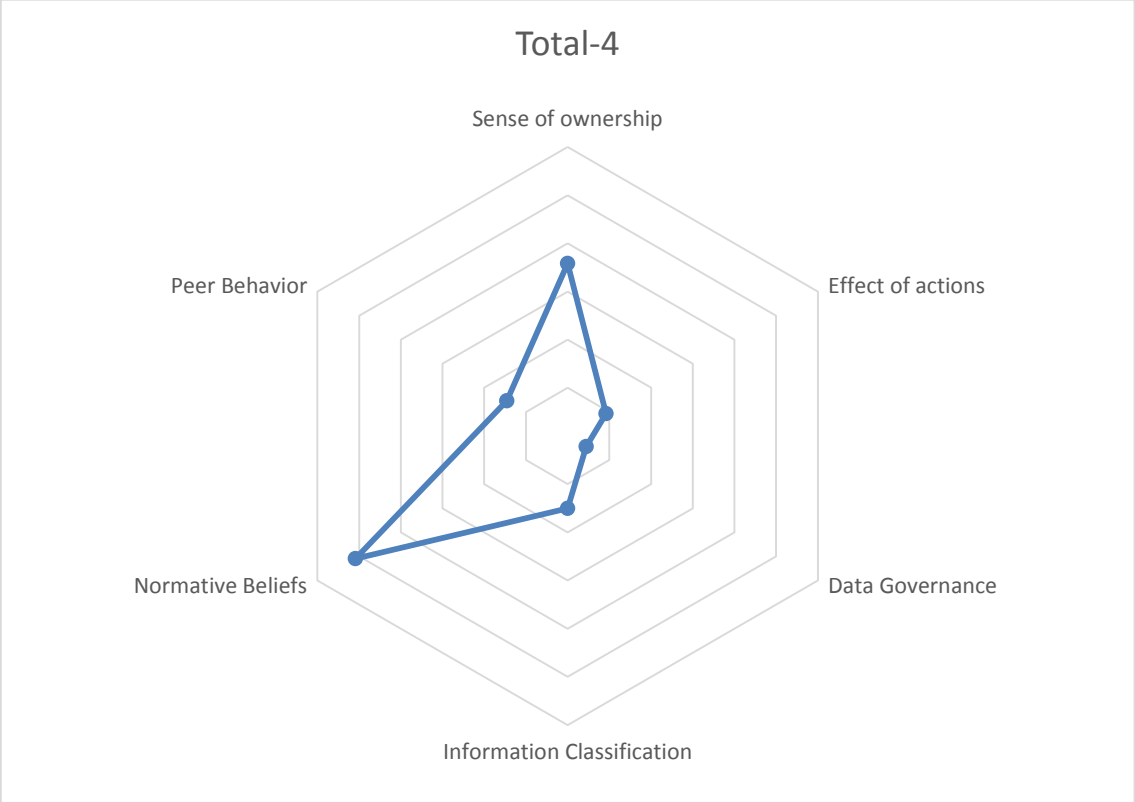


Figure 28 Path coefficients for total-4 (radar)

Total-4	***R2=***	***40,91%***
Sense of ownership	β =	0,358
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

Table 26 Path coefficients for total-4

The coefficients table is summarized in Table 26. Despite the averaged image of the four contexts there is quite some distinction between the factors which raises the question whether and how much this distinction differs between the four contexts. To answer that question the contexts will be analyzed separately in the next chapters 18.7 till 18.10.

18.5 Correlations analysis (total-4)

Before separately analyzing the four contexts, the correlation analysis of the ISP items and control variables from the total-4 dataset were analyzed. Relevant outcomes and recognized relationships are shown in Table 27. The other control variables (e.g. age) have no significant influence or relationship to ISP.

Item	Variable	Correlation to ISP	Coefficient N=371
Familiarity to ISP	ISP1	Moderate positive	,332**
Appropriate ISP	ISP2	Positive	,298**
Information security comes before getting the job done	ISP6	Moderate positive	,369*

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

Table 27 Correlation items on ISP for total-4

Note: This is also an 'averaged image' which might differ per context! Analyzing the total-4 dataset on correlations of ISP items towards PCI confirms the measurement of these items in the model, before the analysis per context. The scored values on the other items provide a generalized view on these items over the 4 contexts.

Individuals' behavior is strongly influenced by situational forces (Pierce et al., 2003). Empirical evidence shows that the effects of behavior differ, for example from sector to sector. Therefore, the conclusions of the research are only applicable to the sector/context the research took place in (Cheng, Li, Li, Holm, & Zhai, 2013; Hovav & D'Arcy, 2012).

The ISP variables measure the perception of end-users on the status of the ISP within their organization in relation to their intentions to comply to PCI. But beware, this doesn't necessarily give an opinion on the status of the ISP itself. Before answering the ISP questions, the participants are stated: "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."

Some notable outcomes of the total-4 dataset correlation to PCI analysis:

- ISP1: Being familiar to the ISP is statistically significant, moderate positively (r=.332, p < 0.01) associated with PCI. This confirms the question which stems from the idea that an end-user should be familiar with ISP before being able to comply (Ifinedo, 2014; NEN-ISO-27002, 2013).
- ISP2: Finding the ISP 'appropriate' is statistically significant, positively (r=.298, p= <0.01) associated with PCI. This confirms the question which stems from the idea that it helps to comply once an end-user can associate itself with an ISP (Albrechtsen, 2007; Posthumus & Von Solms, 2004).
- ISP6: A very positive finding on attitude towards compliance! The statement: "Information security comes before getting the job done" (original statement in questionnaire was inversely stated: "Getting my job done comes before information security") is statistically significant, moderate positively (r=.369, p= <0.05) associated with PCI. This gives a positive view on the 'conflict of interest' discussion from paragraph 2.5 (Ifinedo, 2012; Siponen & Vance, 2010).

More specific insights in the values measured for the different contexts are shown in Figure 29. On the scale 1 till 5 the different contexts have varying mean scores on ISP1, 2 and 6 values.

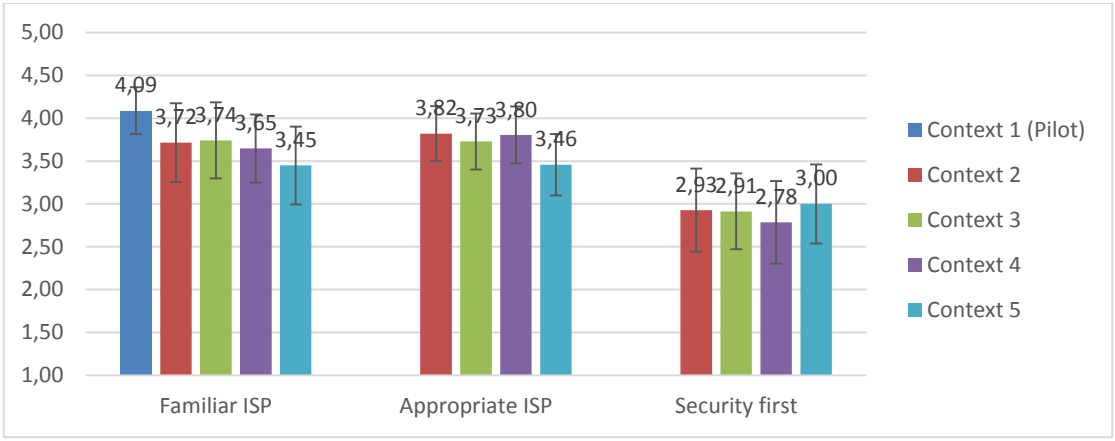


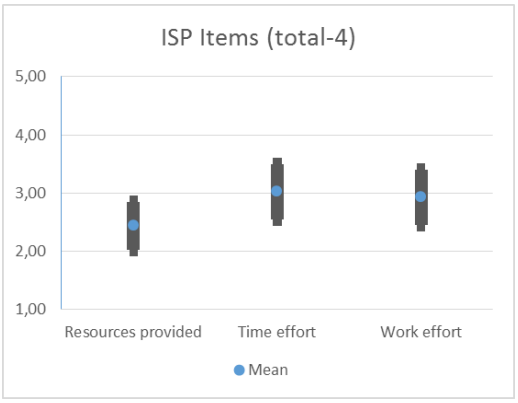
Figure 29 Context ISP status overview

18.6 Further analysis (total-4)

The values returned on the other ISP items provide insights in the attitude of end-users towards their possibilities to comply to policy in the light of provided resources and the time/work effort needed to comply.

Item	Variable	Mean value	Standard dev N=371
Resources provided needed to comply	ISP3	2,44	0,81
Time effort to comply	ISP4	3,03	0,95
Work effort to comply	ISP5	2,93	0,93

Table 28 Value items on ISP for total-4



5 = Strongly agree
4 = Agree
3 = Neutral
2 = Disagree
1 = Strongly disagree

Figure 30 Value items on ISP for total-4

The measured values of total-4 (generalized view of 4 contexts) are listed in Table 28 and graphed in Figure 30. In the graph the mean values are shown together with the standard deviation. These values don't differ significantly per context and provided insights apply to all four measured contexts for these items.

The respondents do not agree on the fact that the resources needed to comply to policy are provided. In context 5 this value is the highest of all contexts, but with a value of 2,69 still below the neutral level meaning that end-users are not provided the resources needed to facilitate the desired behavior of compliance (Ifinedo, 2014).

A more positive finding is in the values on time and work effort needed to comply. Within all contexts these values are more or less on the neutral level. This leaves less opportunity for end-users to excuse on work pressure in case of non-compliance (Siponen & Vance, 2010).

18.7 Analyse context 2

This chapter reports the analysis of the context and does not yet express findings or conclusions.

A multiple regression analysis was conducted on the specific context to examine the predictors of the Policy Compliance Intention factor for that context. Six predictors were simultaneously entered into the model. Together, the predictors account for 43% (adjusted R2 = 42,78) of the variance in PCI (Policy Compliance Intention). Figure 31, Figure 32 and Table 29 show the measured path coefficients for this context.

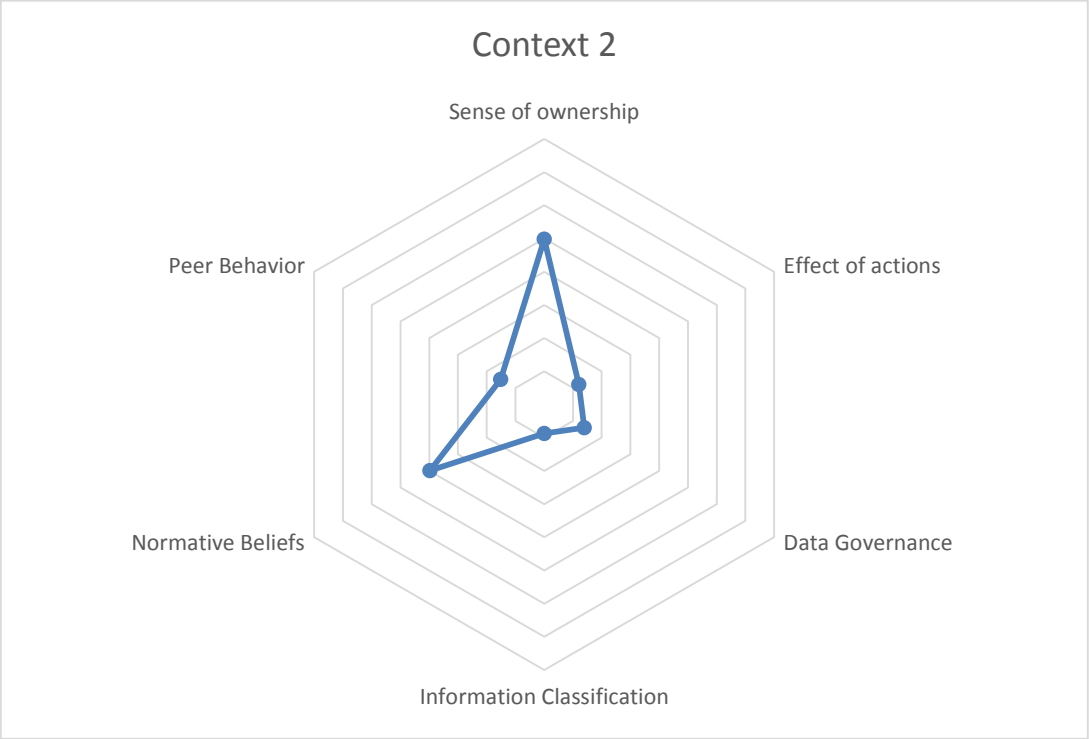


Figure 31 Path coefficients for context 2 (radar)

Context 2	***R2=***	***42,78%***
Sense of ownership	β =	0,498
Effect of actions	β =	0,120
Data Governance	β =	0,139
Information Classification	β =	0,087
Normative Beliefs	β =	0,398
Peer Behavior	β =	0,152

Table 29 Path coefficients for context 2

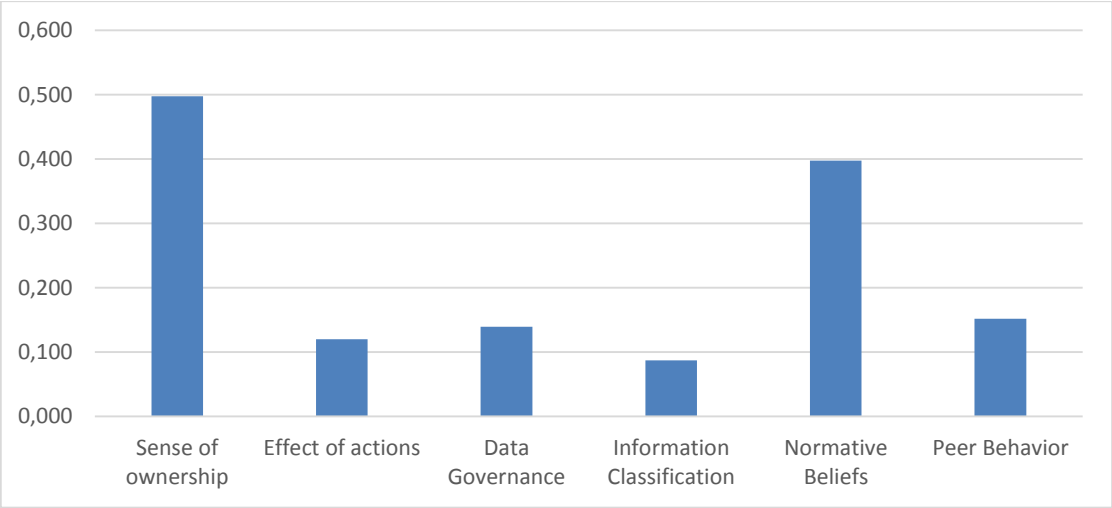


Figure 32 Path coefficients for context 2 (bars)

The findings reported for this context support the hypothesis for the final conceptual model as stated in chapter 15. Positive influences on all hypothesized relationships are found in the research findings shown in Table 30:

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

Table 30 Results on hypothesis for context 2

The correlation analysis for the ISP items for this context are shown in Table 31.

Item	Variable	Correlation	Coefficient N=123
Familiarity to ISP	ISP1	Strong positive	,481**
Appropriate ISP	ISP2	Strong positive	,473**
Information security comes before getting the job done	ISP6	Strong positive	,564**

***. Correlation is significant at the 0.01 level (2-tailed).*

Table 31 Correlation items on ISP for context 2

- ISP1: Being familiar to the ISP is statistically significant, strong positive (r=.481, p < 0.01) associated with PCI.
- ISP2: Finding the ISP 'appropriate' is statistically significant, strong positive (r=.473, p= <0.01) associated with PCI.
- ISP6: Information security comes before getting the job done is statistically significant, strong positive (r=.564, p= <0.01) associated with PCI.

18.8 Analyse context 3

This chapter reports the analysis of the context and does not yet express findings or conclusions.

A multiple regression analysis was conducted on the specific context to examine the predictors of the Policy Compliance Intention factor for that context. Six predictors were simultaneously entered into the model. Together, the predictors account for 29% (adjusted R2 = 28,93) of the variance in PCI (Policy Compliance Intention). Figure 33, Figure 34 and Table 32 show the measured path coefficients for this context.

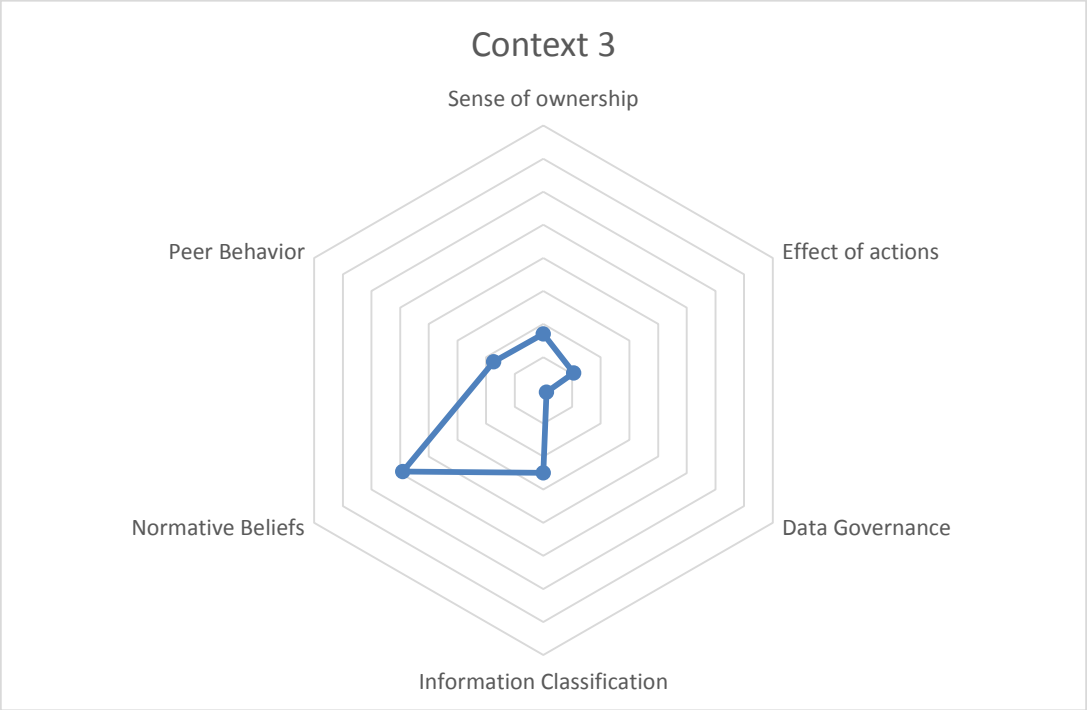


Figure 33 Path coefficients for context 3 (radar)

Context 3	***R2=***	***28,93%***
Sense of ownership	β =	0,170
Effect of actions	β =	0,106
Data Governance	β =	0,011
Information Classification	β =	0,250
Normative Beliefs	β =	0,491
Peer Behavior	β =	0,173

Table 32 Path coefficients for context 3

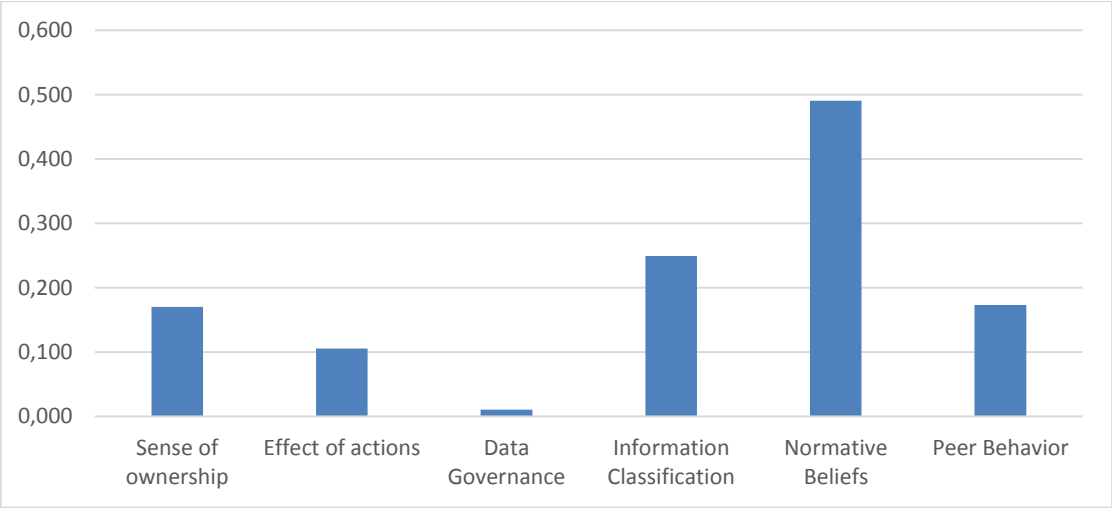


Figure 34 Path coefficients for context 3 (bars)

The findings reported partly support the hypothesis for the final conceptual model as stated in chapter 15. Positive influences on five out of six hypothesized relationships are found in the research findings shown in Table 33:

Nr.	Hypothesis	Result
H1a+	Data Governance positively influences PCI	No support
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

Table 33 Results on hypothesis for context 3

The correlation analysis for the ISP items for this context are shown in Table 34.

Item	Variable	Correlation	Coefficient N=81
Familiarity to ISP	ISP1	Positive	,299**
Appropriate ISP	ISP2	Positive	,242*
Information security comes before getting the job done	ISP6	Strong positive	,415**

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

Table 34 Correlation items on ISP for context 3

- ISP1: Being familiar to the ISP is statistically significant, positive (r=.299, p < 0.01) associated with PCI.
- ISP2: Finding the ISP 'appropriate' is statistically significant, positive (r=.242, p= <0.05) associated with PCI.
- ISP6: Information security comes before getting the job done is statistically significant, strong positive (r=.415, p= <0.01) associated with PCI.

18.9 Analyse context 4

This chapter reports the analysis of the context and does not yet express findings or conclusions.

A multiple regression analysis was conducted on the specific context to examine the predictors of the Policy Compliance Intention factor for that context. Six predictors were simultaneously entered into the model. Together, the predictors account for 63% (adjusted R2 = 62,65) of the variance in PCI (Policy Compliance Intention). Figure 35, Figure 36 and Table 35 show the measured path coefficients for this context.

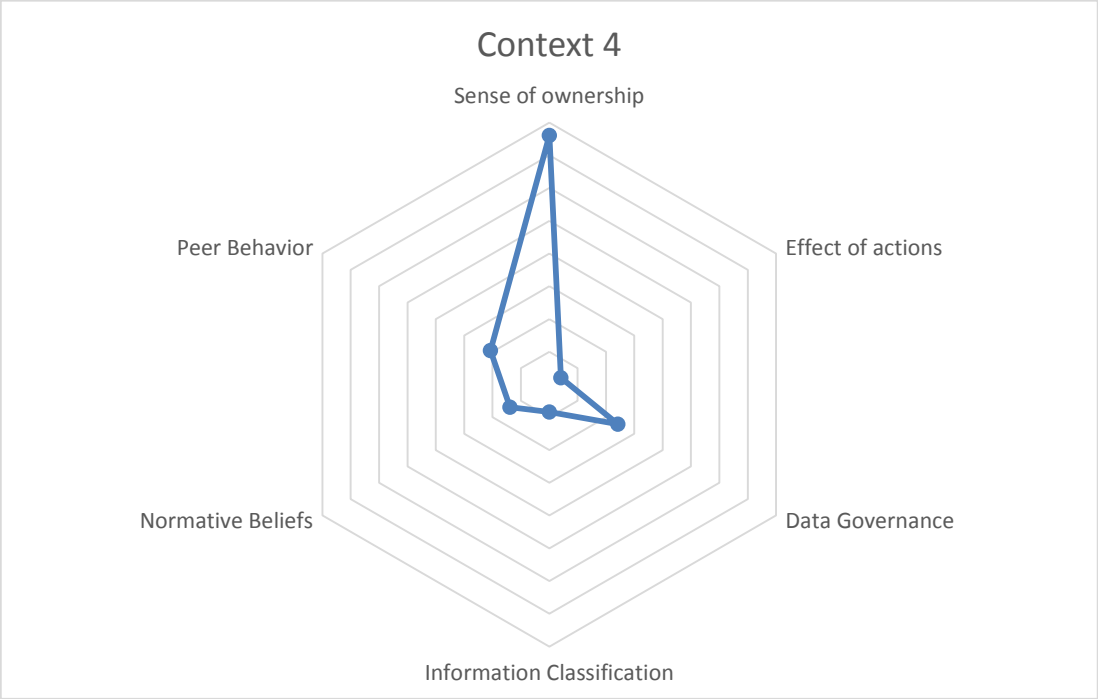


Figure 35 Path coefficients for context 4 (radar)

Context 4	***R2=***	***62,65%***
Sense of ownership	β =	0,760
Effect of actions	β =	0,041
Data Governance	β =	0,242
Information Classification	β =	0,084
Normative Beliefs	β =	0,138
Peer Behavior	β =	0,207

Table 35 Path coefficients for context 4

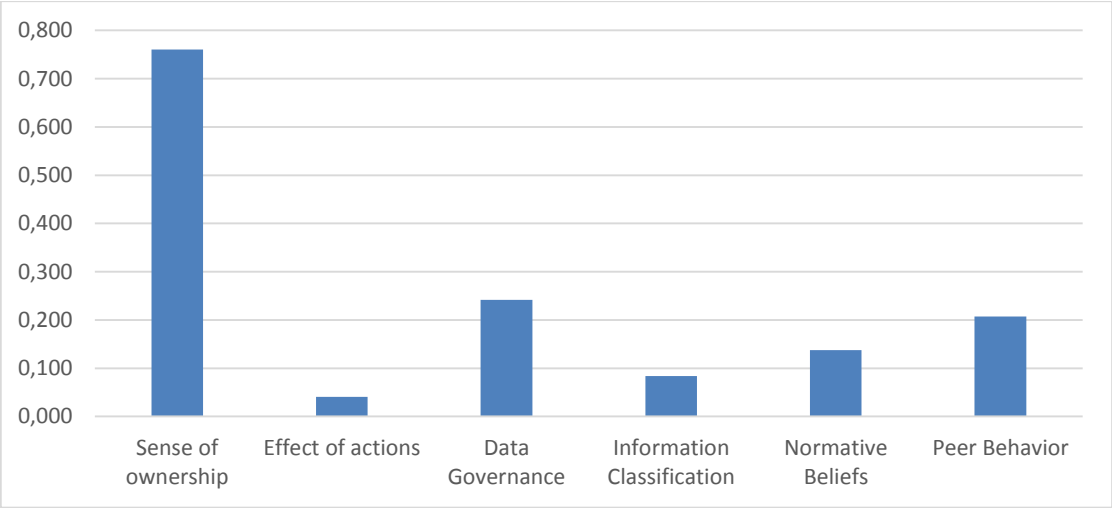


Figure 36 Path coefficients for context 4 (bars)

The findings reported partly support the hypothesis for the final conceptual model as stated in chapter 15. Positive influences on four out of six hypothesized relationships are found in the research findings shown in Table 36:

Nr.	Hypothesis	Result
H1a+	Data Governance positively influences PCI	Supported
H1b+	Information Classification positively influences PCI	No support
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	No support

Table 36 Results on hypothesis for context 4

The correlation analysis for the ISP items for this context are shown in Table 37.

Item	Variable	Correlation	Coefficient N=51
Familiarity to ISP	ISP1	Not supported	,118
Appropriate ISP	ISP2	Not supported	,219
Information security comes before getting the job done	ISP6	Not supported	,179

Table 37 Correlation items on ISP for context 4

None of the correlation items are supported within this context because of the low number of respondents. The coefficients do indicate some level of correlation.

18.10 Analyse context 5

This chapter reports the analysis of the context and does not yet express findings or conclusions.

A multiple regression analysis was conducted on the specific context to examine the predictors of the Policy Compliance Intention factor for that context. Six predictors were simultaneously entered into the model. Together, the predictors account for 36% (adjusted R2 = 36,25) of the variance in PCI (Policy Compliance Intention). Figure 37, Figure 38 and Table 38 show the measured path coefficients for this context.

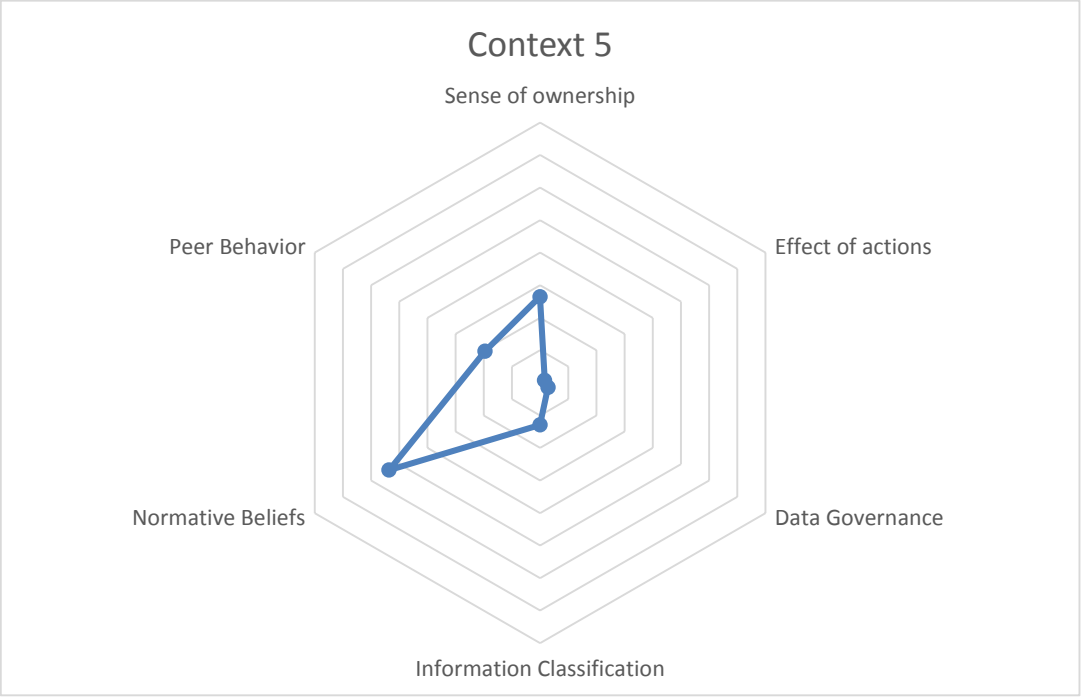


Figure 37 Path coefficients for context 5 (radar)

Context 5	***R2=***	***36,25%***
Sense of ownership	β =	0,265
Effect of actions	β =	0,016
Data Governance	β =	0,028
Information Classification	β =	0,129
Normative Beliefs	β =	0,536
Peer Behavior	β =	0,195

Table 38 Path coefficients for context 5

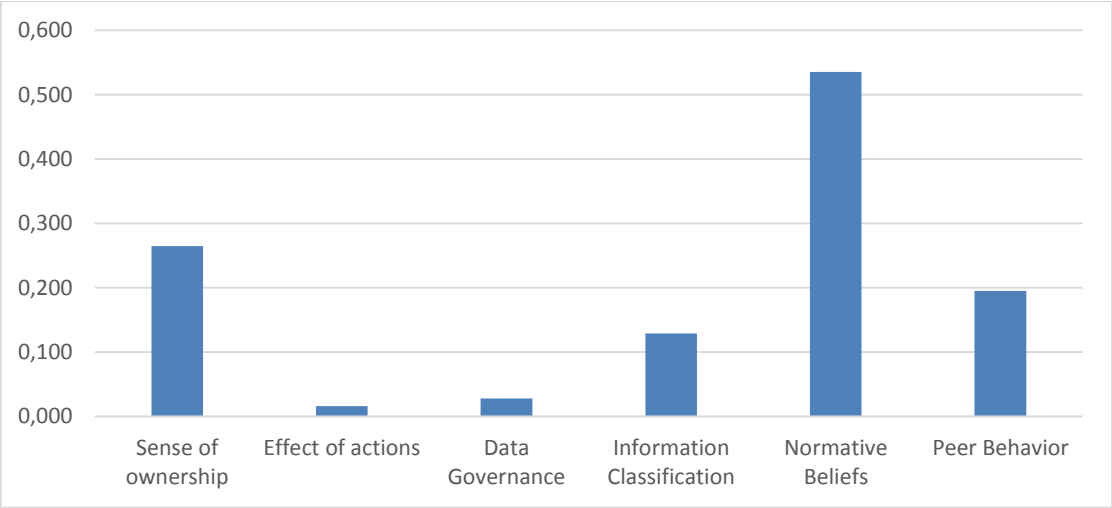


Figure 38 Path coefficients for context 5 (bars)

The findings reported partly support the hypothesis for the final conceptual model as stated in chapter 15. Positive influences on four out of six hypothesized relationships are found in the research findings shown in Table 39:

Nr.	Hypothesis	Result
H1a+	Data Governance positively influences PCI	No support
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	No support

Table 39 Results on hypothesis for context 5

The correlation analysis for the ISP items for this context are shown in Table 40.

Item	Variable	Correlation	Coefficient N=116
Familiarity to ISP	ISP1	Positive	,220*
Appropriate ISP	ISP2	Not supported	,146
Information security comes before getting the job done	ISP6	Not supported	,127

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

Table 40 Correlation items on ISP for context 5

- ISP1: Being familiar to the ISP is statistically significant, positive (r=.220, p < 0.05) associated with PCI.

The other correlation items are not supported within this context because of low significance. The coefficients do indicate some level of correlation.

18.11 Combined view of contexts

Back to the pattern of the averaged image to keep in mind as requested in chapter 18.4. As a reminder, the same image of total-4 is shown below as Figure 39:

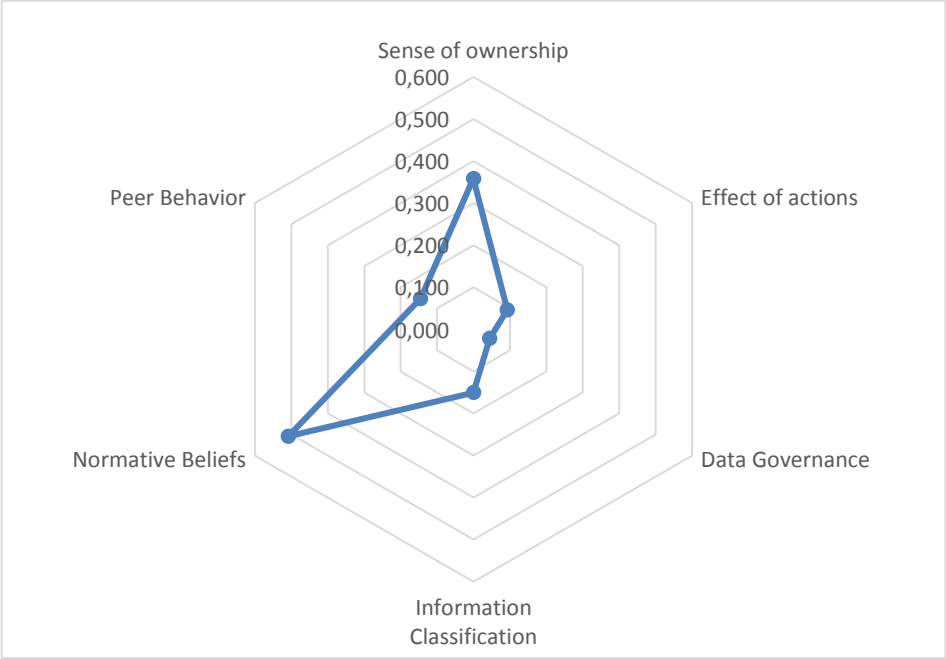


Figure 39 Generalized pattern (repeated)

Looking at Figure 40 below, which shows the radar plots of all 5 contexts (including the pilot context), the same generalized pattern is seen at first sight. But into more detail a remarkable finding is shown where can be seen that the relevance per context is levelled out in the generalized pattern of Figure 39 and the factors measure quite different per context.

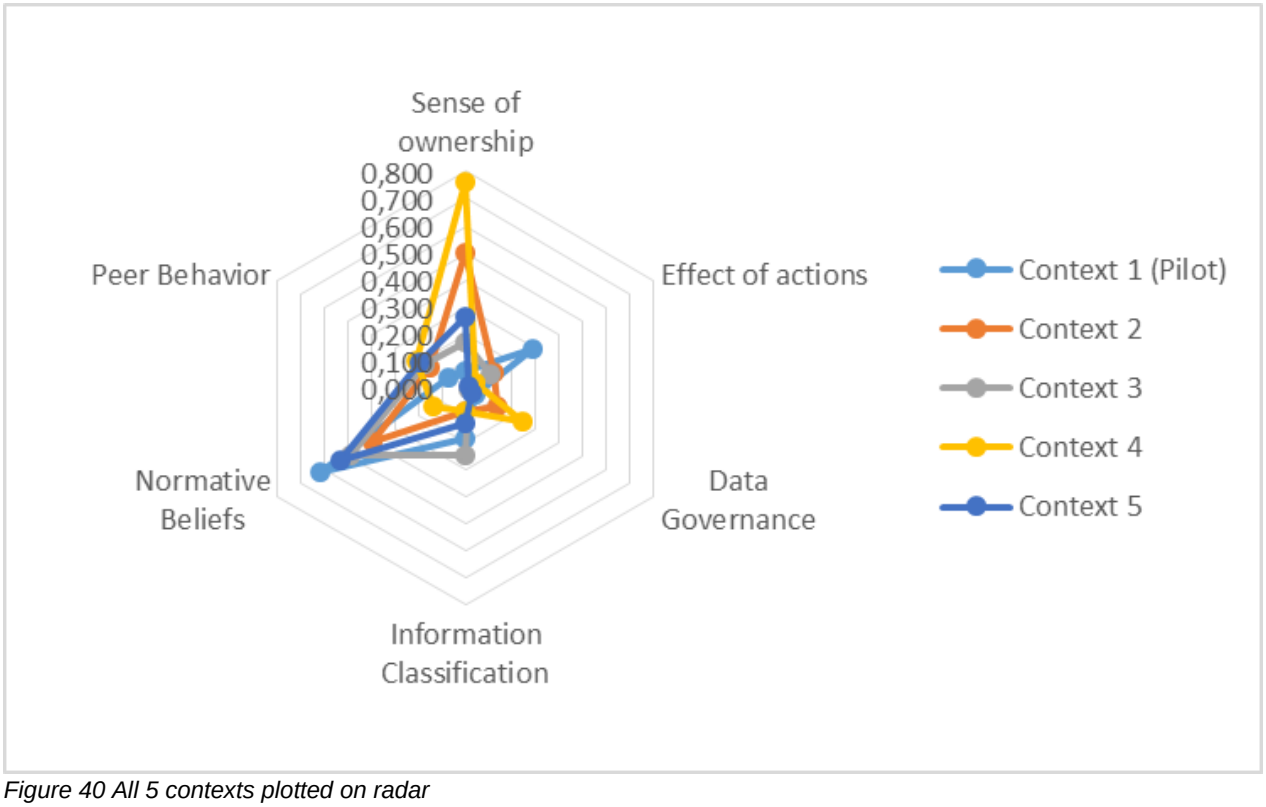
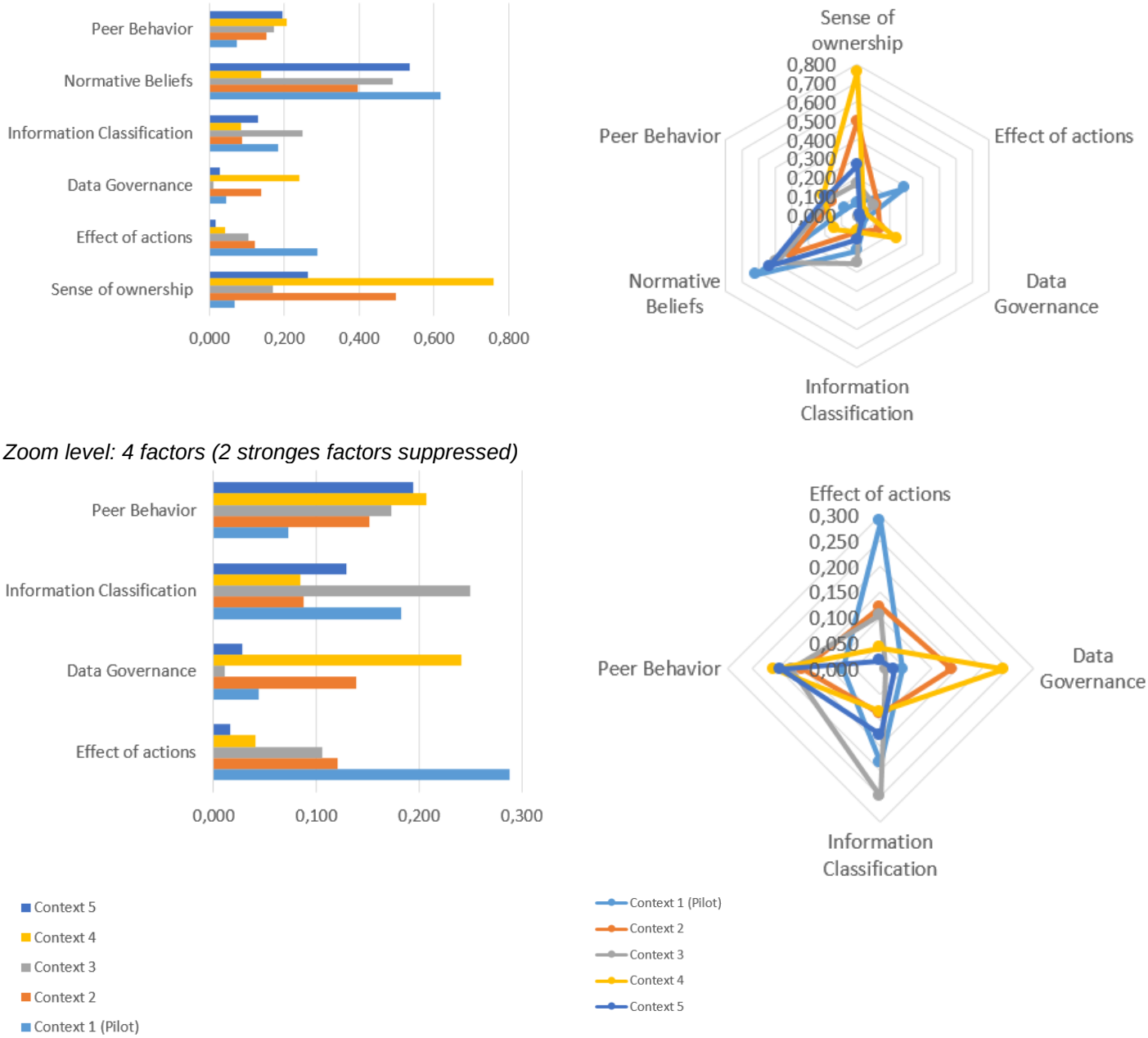


Figure 40 All 5 contexts plotted on radar

18.12 Context comparisons

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 41.

Zoom level: 6 factors



Zoom level: 4 factors (2 stronges factors suppressed)

Figure 41 Comparison of contexts

These insights lead to the main finding on the path analysis: There lies a certain value in the generalized view on the motivational factors, but the motivational factors should be measured per context if an organization needs targeted advice on their organization specific security program.

Herath & Rao (2009b) did not measure per context but provided a generalized view on the roles they researched. This makes the insights learned from this thesis an important addition to their work.

19 Conclusion and Recommendations (Output 4)

This chapter will combine all findings and report conclusions and recommendations. Starting with the research question as stated in chapter 4:

What motivational factors relate, in which degree, to intentions on compliance and how could these insights be utilized to promote end-users compliance to ISP within a given organization?

The research question is answered in three parts:

Part 1: *What motivational factors relate to intentions on compliance?*
From literature review (§ 6) the conceptual model (§ 7) is formed. Both are judged and refined using SME sessions (§ 8). The proposed model (§ 9) provided the starting point for designing a survey instrument (§ 10) from which a pilot is conducted (§ 11) and analyzed (§ 12 & 13). The final research instrument (§ 14) is based on the final conceptual model (§ 15). The final model shows a total of six motivational factors which relate to intentions on compliance to be utilized to promote end-users compliance to ISP within a given organization. These are listed below:

Intrinsic motivational factors:
- Sense of ownership
- Effect of actions

Extrinsic motivational factors:
- Data Governance
- Information Classification
- Normative Beliefs
- Peer Behavior

Part 2: *In which degree do these motivational factors relate within a given organization?*
Using the final research instrument, surveys are conducted within four organizations / contexts (§ 16). These measurements (§ 17) are analyzed (§ 18). The degree to which these motivational factors relate show certain similarities but at the same time differs per context. Additional findings are reported (Appendix G). A summary is found in Figure 42 below showing degrees per context and Figure 43 showing an averaged view of degrees for context 2 till 5:

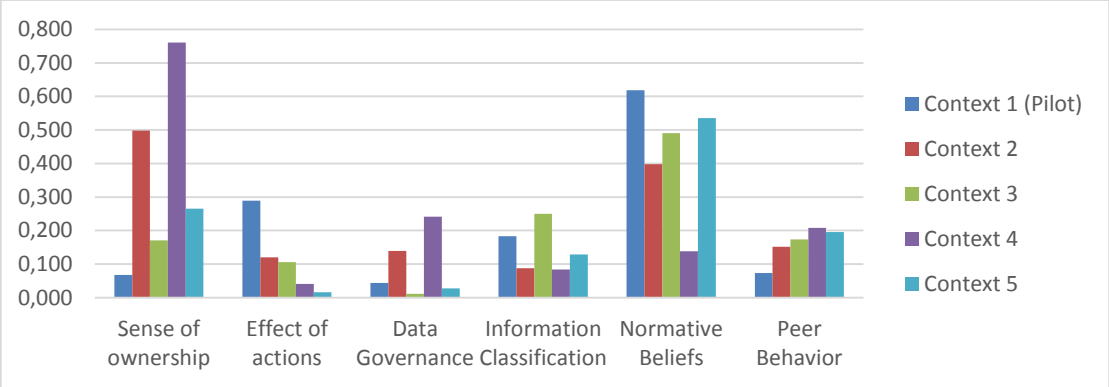


Figure 42 Summary of degrees

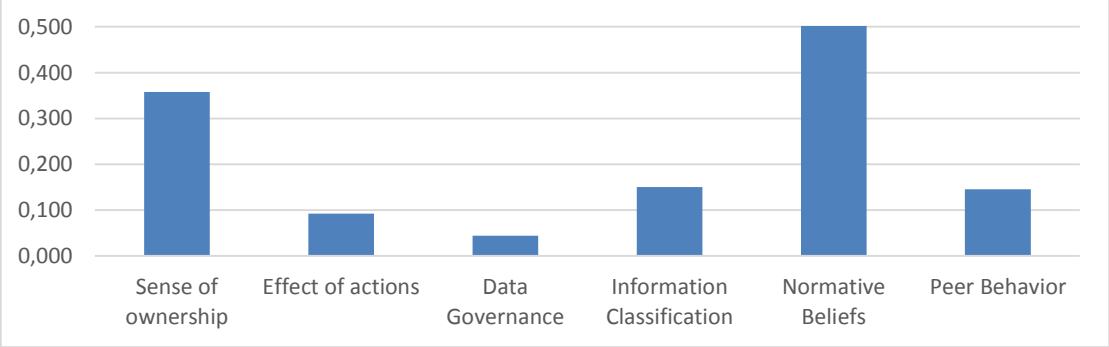


Figure 43 Averaged view of degrees

The generalized findings reported support the hypothesis for the final conceptual model as stated in chapter 15. As expected, in general, positive influences on all hypothesized relationships are found in the research findings shown in Table 41:

Nr.	Hypothesis	Result
H1a+	Data Governance positively influences PCI	Supported (3 out of 5)
H1b+	Information Classification positively influences PCI	Supported (4 out of 5)
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 (3 out of 5)

Table 41 Results on hypothesis

Part 3: *How could these insights be utilized to promote end-users compliance to ISP?*

Motivational factors with a relation to compliance to ISP can be utilized to promote end-users compliance to ISP. Organizations are able to shape conditions likely to promote these specific motivational factors (Ajzen, 1991; Ifinedo, 2014; Ryan & Deci, 2000a; Stanton et al., 2005; Weber et al., 2009). Suggestions on how to utilize these factors are found in paragraph 19.1.

19.1 Conclusions

From the answered research question the following conclusion are drawn:

Conclusion 1) From the findings of the research is concluded that in general "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 the conditions to shape should have its 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. Normative beliefs are based on the belief as to whether or not a significant person wants the end-user to perform the expected behavior (Bulgurcu et al., 2010; Herath & Rao, 2009b; Ifinedo, 2014).

Conclusion 2) From the findings of the research is concluded that in general "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 the conditions to shape should have its focus on empowering and allowing end-users to exercise a certain level of control over important aspects of their work arrangements. Aspects like job satisfaction and self-esteem improve sense of ownership (Avey et al., 2009; Van Dyne & Pierce, 2004; Mayhew, Ashkanasy, Bramble, & Gardner, 2007; Spears & Barki, 2010).

Conclusion 3) From the findings of the research is concluded that the four other motivational factors should first be measured within the specific organization context to determine their relevance to that context. Measurements show that some of these factors are missing any relevance for a specific context but do show significant relevance for another 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 effective within that context.

Suggestions to utilize these insights in practice follow for each factor:

- Effect of actions, as an intrinsic motivational factor, can be utilized in practice if conditions to shape by the specific organization have focus 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 & Rao, 2009b; Olckers, 2013).

- Data governance, as an extrinsic motivational factor, can be utilized in practice if conditions to shape have focus 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 & Chang, 2007; Lee & Strong, 2003; NEN-ISO-27002, 2013; Weber et al., 2009).

- Information Classification, as an extrinsic motivational factor, can be utilized in practice if conditions to shape have focus 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. Applying includes 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 & Hale, 2009; Puhakainen & Siponen, 2010; Veiga & Eloff, 2007).

- Peer behavior, as an extrinsic motivational factor, can be utilized in practice if conditions to shape have focus 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, & Kallgren, 1990). End-users seeing their co-workers routinely follow ISP are likely to carry out similar behaviors (Cheng et al., 2013; Cialdini et al., 1990; Fishbein & Ajzen, 1975; Herath & Rao, 2009a, 2009b).

Additional findings from the research are reported in Appendix G (Additional findings).

19.2 Recommendations

As reported in chapter 16 the reason for most organizations to not participate in the survey was found in the 'timing' of the research. Once an organization has the priority, capability and capacity to follow up on the measurement the 'timing' is 'correct'. In such cases the instrument developed by this thesis provides the needed insights before starting, for example a compliance campaign, making it possible to focus on the most effective motivational factors. At the same, insight is provided in the status of the ISP, making it possible to effectuate such campaign from two principles:

- promoting motivational factors by shaping conditions
- improving familiarity to ISP

The measurement of the context using the instrument developed within this thesis provides the needed insights for the specific organization and translates the measurements into applicable practical advices to use within such campaign or security program.

Independent of the timing and practical relevance as described above, there is also more general scientific relevance in the outcomes of this thesis. From the outcomes is concluded that shaping conditions around "normative beliefs" and "sense of ownership" always provides of positive influence to compliance, despite the context.

To further enhance these recommendations more insights and knowledge on the motivational factors could be gained in case the instrument is applied to more contexts within the same segment / field of work. Such research could provide further insights on the specific motivational factors and their relevance within a segment. There's a possibility these insights help shaping conditions for specific segments leaving out the effort of measuring a specific context in advance of a campaign or security program.

20 References

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.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security*, *28*(6), 476–490. Elsevier Ltd.

Amabile, T. M. (1993). Motivational Synergy: Toward new conceptualizations of intrinsic and extrinsic motivation in the workplace. *Human Resources Management Review*, *3*(3), 185–201.

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.

Baruch, Y. (1999). Response rate in academic studies: a comparative analysis. *Human Relations*, *52*(4), 421–438.

Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human Relations*, *61*(8), 1139–1160.

Bojanc, R., & Jerman-Blažič, B. (2013). A Quantitative Model for Information-Security Risk Management. *Engineering Management Journal*, *25*(2), 25–37.

Bryman, A., & Bell, E. (2007). *Business Research Methods*. *Social Research*.

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.

CA Technologies. (2014). *Identity-centric security*. Retrieved from http://www.ca.com/us/~/media/Files/SolutionBriefs/identity-centric-security-the-ca-identity-and-access-management-suite.pdf

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*.

Clinch, J. (2009). Itil v3 and information security. *Clinch Consulting White Paper*, (May), 1 – 40.

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

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*.

Fyffe, G. (2008). Addressing the insider threat. *Network Security*.

Gliem, J. a, & Gliem, R. R. (2003). Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales,. *2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education*, (1992), 82–88.

Gordon, L. a., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457.

Grant, A. M. (2008). Does intrinsic motivation fuel the prosocial fire? Motivational synergy in predicting persistence, performance, and productivity. *The Journal of applied psychology*, *93*(1), 48–58.

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.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

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

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information and Management*, *49*(2), 99–110. Elsevier B.V.

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.

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.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security*, *27*, 224–231.

Lee, Y. W., & Strong, D. M. (2003). Knowing-Why About Data Processes and Data Quality. *Journal of Management Information Systems*, *20*(3), 13–39.

Leung, S.-O. (2011). A Comparison of Psychometric Properties and Normality in 4-, 5-, 6-, and 11-Point Likert Scales. *Journal of Social Service Research*.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of psychology*.

Lin, H.-F. (2007). Effects of extrinsic and intrinsic motivation on employee knowledge sharing intentions. *Journal of Information Science*, *33*(2), 135–149.

Loch, K., Carr, H., & Warkentin, M. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, *June*, 173–186.

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*.

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/

Ponemon Institute. (2015). *2015 State of the Endpoint Report : User-Centric Risk*. Retrieved from http://www.ponemon.org/local/upload/file/2015 State of Endpoint Risk FINAL.pdf

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers and Security*, *23*, 638–646.

Preston, C. C., & Colman, a M. (2000). Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta psychologica*, *104*(1), 1–15.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757–778.

Von Roessing, R. M. (2010). *The Business Model for Information Security*. *Information Security*.

Ryan, R., & Deci, E. (2000a). Self-determination theory and the facilitation of intrinsic motivation. *American Psychologist*, *55*(1), 68–78.

Ryan, R., & Deci, E. (2000b). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary educational psychology*, *25*(1), 54–67.

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society*, *31*(June), 24–29.

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.

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

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*, 371–376.

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.

Thomson, K., & Solms, R. Von. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud Security*, *2006*(May), 11–15.

Thomson, K.-L., Solms, R. Von, & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(October), 7–11.

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

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3-4), 190–198. Elsevier B.V.

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

Verizon. (2014a). *2014 Data Breach Investigation Report*. Retrieved from http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

Verizon. (2014b). *2014 Data Breach Investigations Report Executive Summary*. Retrieved from http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

Warkentin, M., & Johnston, A. C. (2008). IT Governance and Organizational Design for Security Management. *Information Security: Policies, Processes and Practices* (pp. 46–68).

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.

Zhao, X., Xue, L., & Whinston, A. (2009). Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling. *International Conference on Information Systems*, *30*(1), 1–17.

21 Abbreviation list

EFA	Exploratory Factor Analysis
FTE	Full Time Equivalent
ICT	Information & Communication Technology
ISP	Information Security Policy / Policies
ISM	Information Security Management
IT	Information Technology
SME	Subject Matter Expert(s)
SPSS	Statistical Package for the Social Sciences

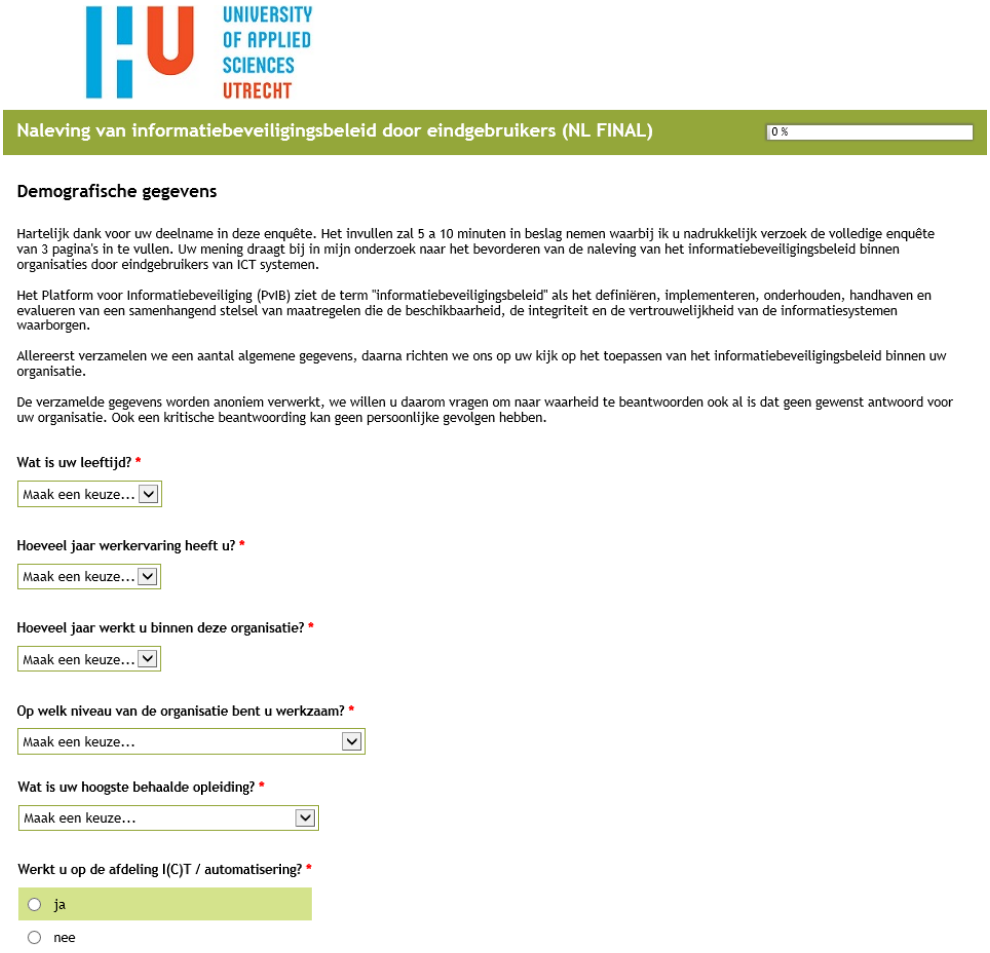
22 Appendices

In the appendices part, the following appendices are found:

23 Appendix A (Final survey instrument)

23.1 Non-global version (in Dutch)

Page 1:



UNIVERSITY OF APPLIED SCIENCES UTRECHT

Naleving van informatiebeveiligingsbeleid door eindgebruikers (NL FINAL) 0 %

Demografische gegevens

Hartelijk dank voor uw deelname in deze enquête. Het invullen zal 5 a 10 minuten in beslag nemen waarbij ik u nadrukkelijk verzoek de volledige enquête van 3 pagina's in te vullen. Uw mening draagt bij in mijn onderzoek naar het bevorderen van de naleving van het informatiebeveiligingsbeleid binnen organisaties door eindgebruikers van ICT systemen.

Het Platform voor Informatiebeveiliging (PvIB) ziet de term "informatiebeveiligingsbeleid" als het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen die de beschikbaarheid, de integriteit en de vertrouwelijkheid van de informatiesystemen waarborgen.

Allereerst verzamelen we een aantal algemene gegevens, daarna richten we ons op uw kijk op het toepassen van het informatiebeveiligingsbeleid binnen uw organisatie.

De verzamelde gegevens worden anoniem verwerkt, we willen u daarom vragen om naar waarheid te beantwoorden ook al is dat geen gewenst antwoord voor uw organisatie. Ook een kritische beantwoording kan geen persoonlijke gevolgen hebben.

Wat is uw leeftijd? *

Maak een keuze...

Hoeveel jaar werkervaring heeft u? *

Maak een keuze...

Hoeveel jaar werkt u binnen deze organisatie? *

Maak een keuze...

Op welk niveau van de organisatie bent u werkzaam? *

Maak een keuze...

Wat is uw hoogste behaalde opleiding? *

Maak een keuze...

Werkt u op de afdeling I(C)T / automatisering? *

- ja
- nee

Page 2:

UNIVERSITY OF APPLIED SCIENCES UTRECHT

Naleving van informatiebeveiligingsbeleid door eindgebruikers (NL FINAL) 33 %

Onderzoek omtrent informatiebeveiligingsbeleid (pagina 2 van 3)

Pagina 2 van 3:
In het volgende deel vraag ik u een aantal stellingen omtrent het informatiebeveiligingsbeleid van uw organisatie te beoordelen. Kies per stelling welk antwoord u het het meest toepasbaar vindt op uw situatie.

Hanteer de volgende uitgangspunten tijdens de beantwoording van de stellingen:
- Als eindgebruiker heeft u een goedaardige insteek, er is geen kwade zin.
- Een informatiebeveiligingsbeleid is altijd aanwezig. Deze hoeft niet formeel te zijn vastgesteld maar kan ook bestaan uit informele afspraken, normen/waarden, uw gevoel of eigen inzicht.

Het informatiebeveiligingsbeleid van uw organisatie *

	helemaal mee oneens	mee oneens	mee eens / niet oneens	mee eens	helemaal mee eens
Ik ben bekend met het geldende informatiebeveiligingsbeleid van mijn organisatie	○	○	○	○	○
Ik vind het geldende beleid toepasselijk voor mijn organisatie	○	○	○	○	○
De (werk)middelen om te kunnen conformeren aan het beleid zijn voor mij verkrijgbaar. Hiermee kan ik mijn taken volgens beleid uitvoeren.	○	○	○	○	○
Mijn werk uitvoeren conform het informatiebeveiligingsbeleid kost me meer tijd	○	○	○	○	○
Mijn werk uitvoeren comform het informatiebeveiligingsbeleid kost me meer moeite	○	○	○	○	○
Mijn werk afkrijgen stel ik op de eerste plaats, vóór informatiebeveiliging	○	○	○	○	○

Wat is uw verwachting van de effectiviteit van een informatiebeveiligingsbeleid *

	helemaal mee oneens	mee oneens	mee eens / niet oneens	mee eens	helemaal mee eens
Elke medewerker kan het verschil maken in de beveiliging van de informatiesystemen van mijn organisatie	○	○	○	○	○
Ik kan het verschil maken in de beveiliging van de informatiesystemen van mijn organisatie	○	○	○	○	○

Beoordeel de rol van de werkomgeving in het opvolgen van het informatiebeveiligingsbeleid *

	helemaal mee oneens	mee oneens	mee eens / niet oneens	mee eens	helemaal mee eens
Mijn directie vindt dat ik het informatiebeveiligingsbeleid van de organisatie moet opvolgen	○	○	○	○	○
Mijn direct leidinggevende vindt dat ik het informatiebeveiligingsbeleid van de organisatie moet opvolgen	○	○	○	○	○
Mijn collega's vinden dat ik het informatiebeveiligingsbeleid van de organisatie moet opvolgen	○	○	○	○	○
De I(C)T afdeling vindt dat ik het informatiebeveiligingsbeleid van de organisatie moet opvolgen	○	○	○	○	○
De staffunctionarissen en adviseurs in mijn organisatie vinden dat het informatiebeveiligingsbeleid moet worden opgevolgd	○	○	○	○	○
Het is voor de hand liggend dat de meeste medewerkers zich aan het informatiebeveiligingsbeleid houden	○	○	○	○	○
Ik veronderstel dat andere medewerkers zich aan het informatiebeveiligingsbeleid houden	○	○	○	○	○
Ik weet zeker dat andere medewerkers zich aan het informatiebeveiligingsbeleid houden	○	○	○	○	○

Page 2 (continued):

Beoordeel uw intenties tot het opvolgen van het informatiebeveiligingsbeleid van uw organisatie *

	helemaal mee oneens	mee oneens	mee eens / niet oneens	mee eens	helemaal mee eens
Het is voor de hand liggend dat ik het informatiebeveiligingsbeleid opvolg	○	○	○	○	○
Ik ben bereid te voldoen aan het informatiebeveiligingsbeleid om de informatiesystemen van mijn organisatie te beschermen	○	○	○	○	○
Ik ben zeker dat ik het informatiebeveiligingsbeleid zal opvolgen	○	○	○	○	○

Page 3:

UNIVERSITY OF APPLIED SCIENCES UTRECHT

Naleving van informatiebeveiligingsbeleid door eindgebruikers (NL FINAL) 67 %

Onderzoek omtrent informatiebeveiligingsbeleid (pagina 3 van 3)

Pagina 3 van 3:
In het volgende deel vraag ik u nog een aantal stellingen omtrent het informatiebeveiligingsbeleid van uw organisatie te beoordelen. Kies wederom per stelling welke antwoord u het het meest toepasbaar vindt op uw situatie.

Nogmaals worden de volgende uitgangspunten gehanteerd tijdens de beantwoording van de stellingen:
- Als eindgebruiker heeft u een goedaardige insteek, er is geen kwade zin.
- Een beleid is altijd aanwezig. Deze hoeft niet formeel te zijn vastgesteld maar kan ook bestaan uit informele afspraken, normen/waarden, uw gevoel of eigen inzicht.

Beoordeel de rol van eigenaarschap in het opvolgen van het informatiebeveiligingsbeleid *

	helemaal mee oneens	mee oneens	mee eens / niet oneens	mee eens	helemaal mee eens
Ik voel mij betrokken bij mijn organisatie	○	○	○	○	○
Ik voel me binnen mijn organisatie op mijn gemak	○	○	○	○	○
Ik bezit de competenties om mijn werk goed te kunnen uitvoeren	○	○	○	○	○
Ik voel de behoefte om mijn informatie af te schermen van gebruik door anderen in de organisatie	○	○	○	○	○
Ik voel de behoefte om de informatie van mijn organisatie af te schermen van gebruik door andere organisaties	○	○	○	○	○

Beoordeel de rol van de besturing in het opvolgen van het informatiebeveiligingsbeleid (zie onderstaande definities) *

LET OP: In onderstaande vragen worden 2 definities gebruikt:
'inhoudelijk bewaker' is een rol in de organisatie welke zorg draagt over de inhoud van de informatie, onder meer op aspecten als kwaliteit en vertrouwelijkheid.
'beheerder' is een rol in de organisatie welke zorg draagt voor de technische aspecten rondom het in bewaring stellen van informatie zoals het beheer van de opslagsystemen.

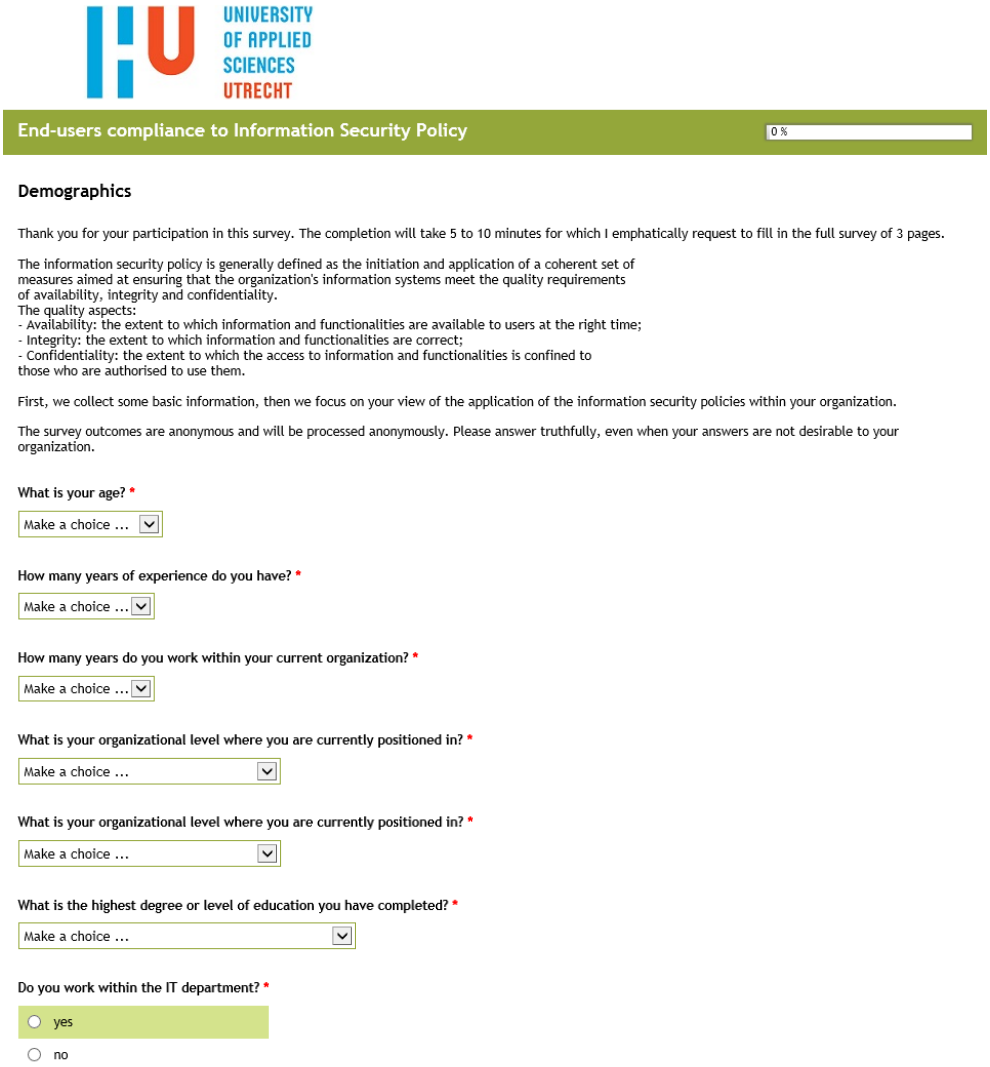
	helemaal mee oneens	mee oneens	mee eens / niet oneens	mee eens	helemaal mee eens
Het helpt mij om informatie te beschermen wanneer een soort van 'inhoudelijk bewaker' zich over de informatie bekommerd	○	○	○	○	○
Ik vind een onderscheid tussen de eigenaar van informatie en de 'inhoudelijke bewaker' over informatie van belang	○	○	○	○	○
Het helpt mij om informatie te beschermen wanneer het 'beheer' van de opslag/informatiesystemen duidelijk is belegd binnen de organisatie	○	○	○	○	○
Ik vind een onderscheid tussen de eigenaar van informatie en de 'beheerder' van opslag/informatiesystemen van belang	○	○	○	○	○
Het helpt mij om informatie te beschermen wanneer er een classificatiesysteem (openbaar, vertrouwelijk, geheim, etc) aanwezig is binnen de organisatie	○	○	○	○	○
Ik vind dat het helder moet zijn welke soort informatie onder een bepaalde classificatie valt	○	○	○	○	○
Ik vind dat het helder moet zijn wat de consequenties van het toekennen van een bepaalde classificatie zijn	○	○	○	○	○

Druk onderaan deze pagina op GEREED om de resultaten op te slaan.

Ik wil u hartelijk bedanken voor uw medewerking!
Hartelijke groet, Peter Straver

23.2 Global version (in English)

Page 1:



UNIVERSITY OF APPLIED SCIENCES UTRECHT

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.	○	○	○	○	○

Page 2 (continued):

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	○	○	○	○	○

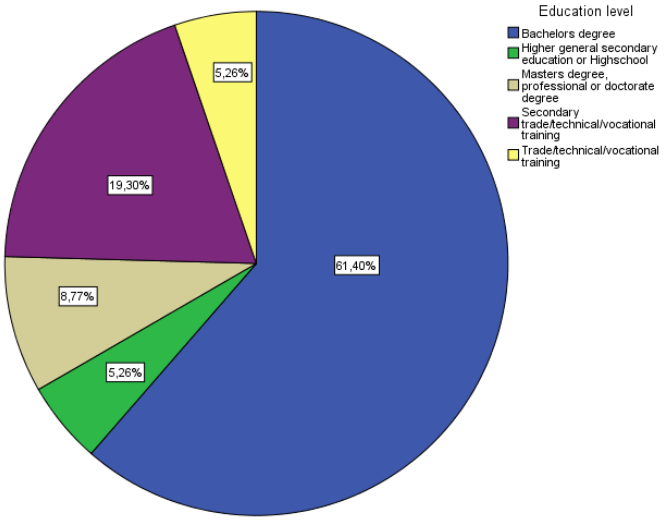
Press DONE at the bottom of this page to store the results.

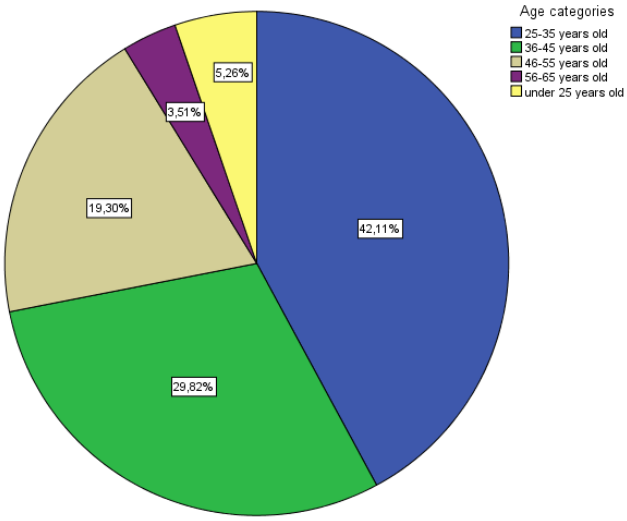
I want to thank you for your cooperation!
Sincerely, Peter Straver

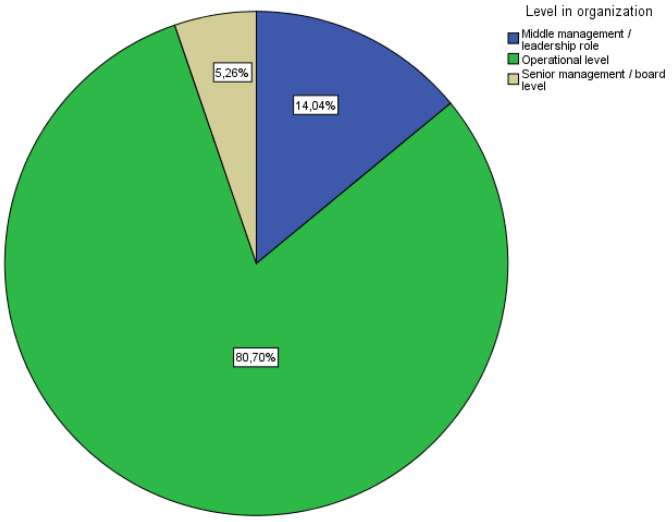
Prev Done

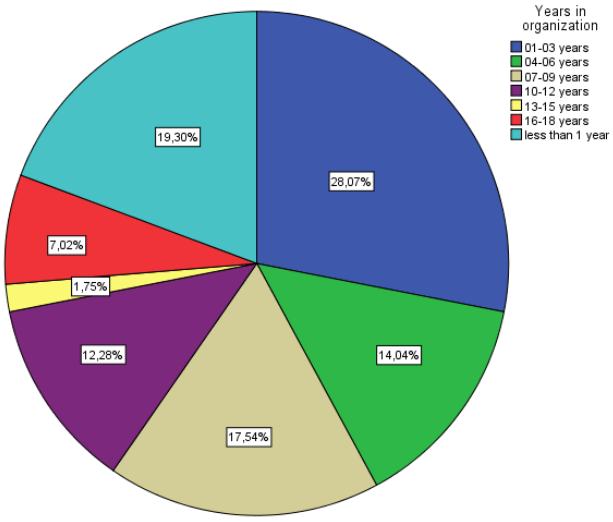
24 Appendix B (Demographics of research context 1)

Below the demographics are shown including a legend per pie diagram.



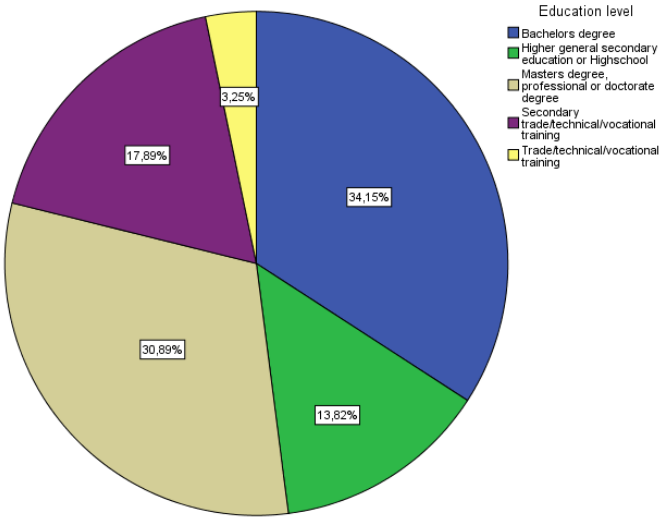


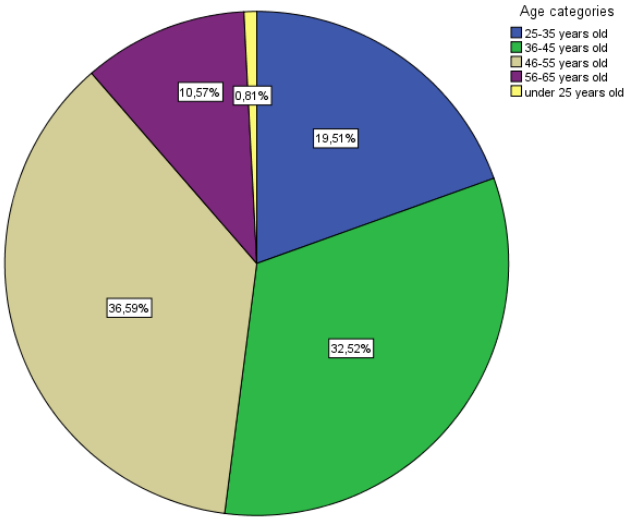


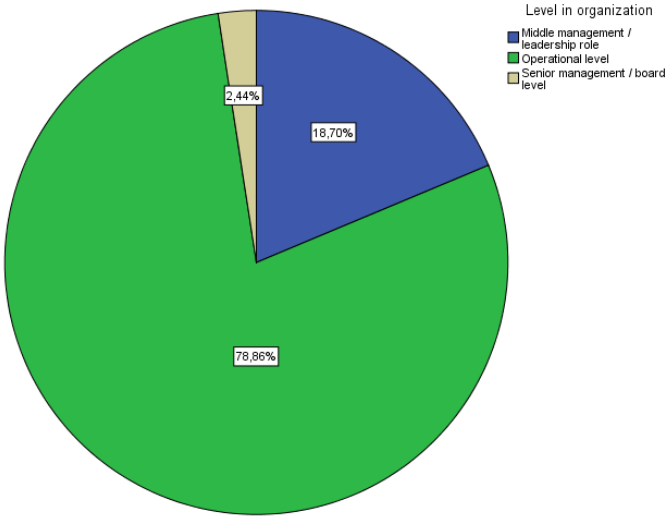


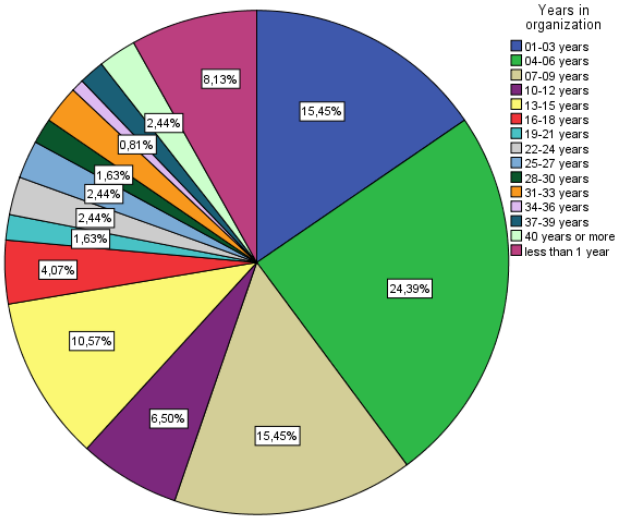
25 Appendix C (Demographics of research context 2)

Below the demographics are shown including a legend per pie diagram.



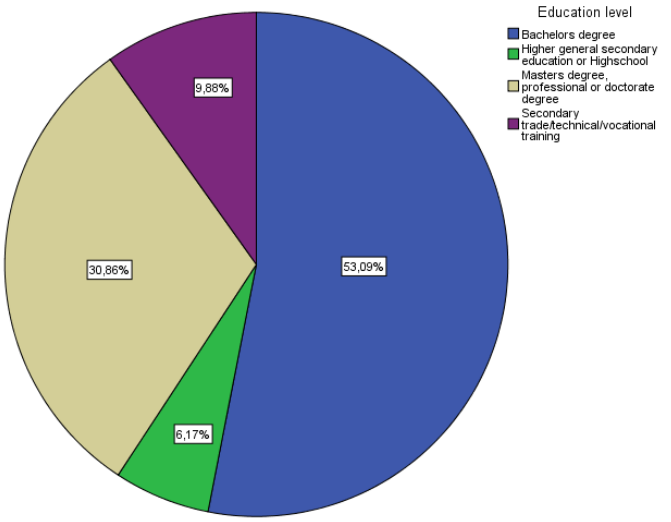


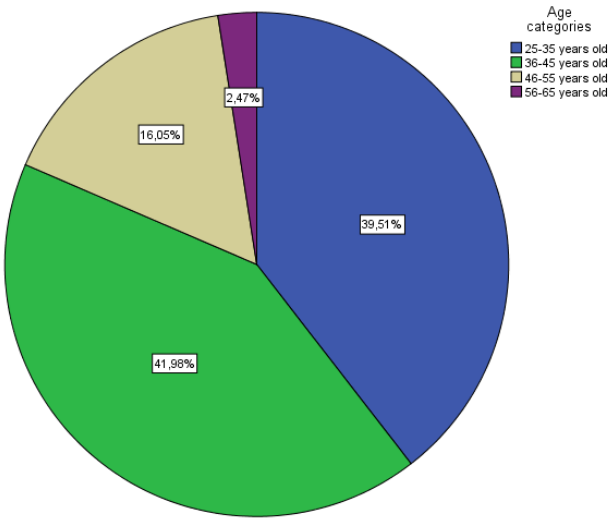


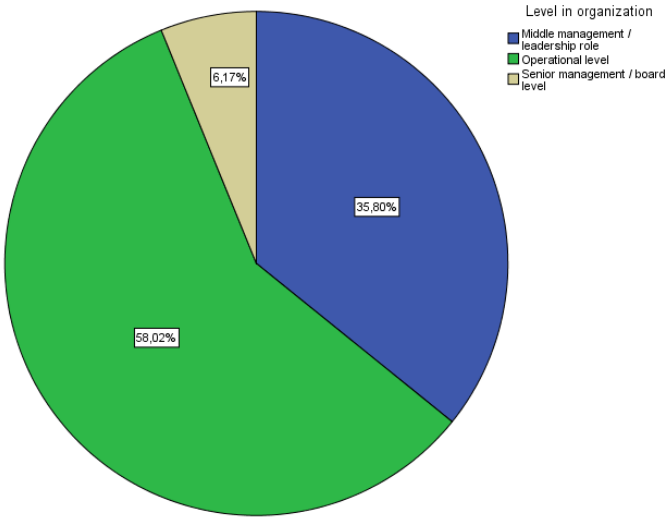


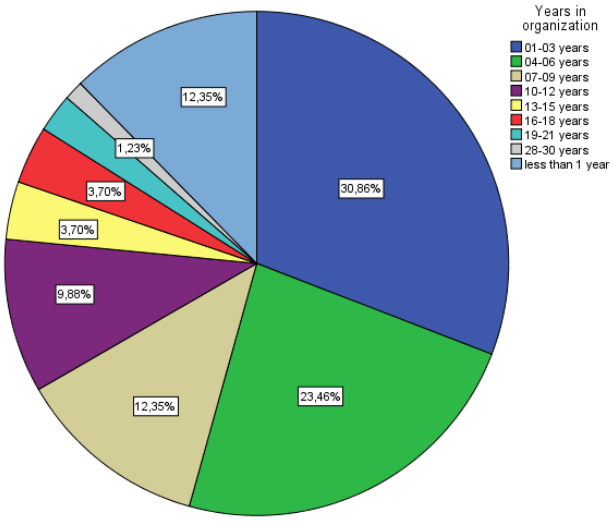
26 Appendix D (Demographics of research context 3)

Below the demographics are shown including a legend per pie diagram.



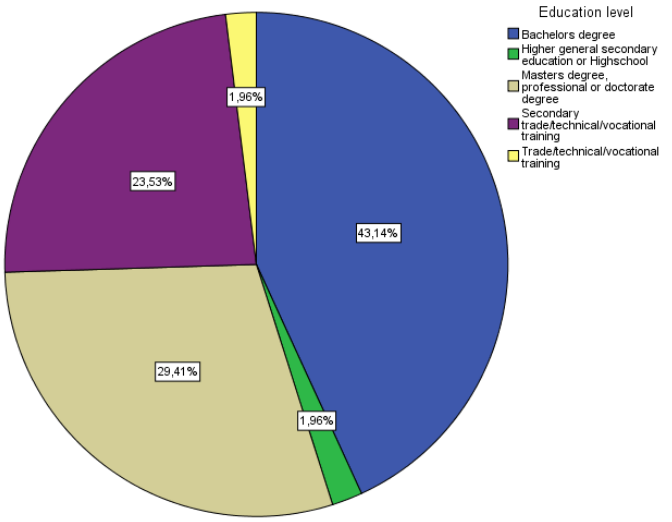


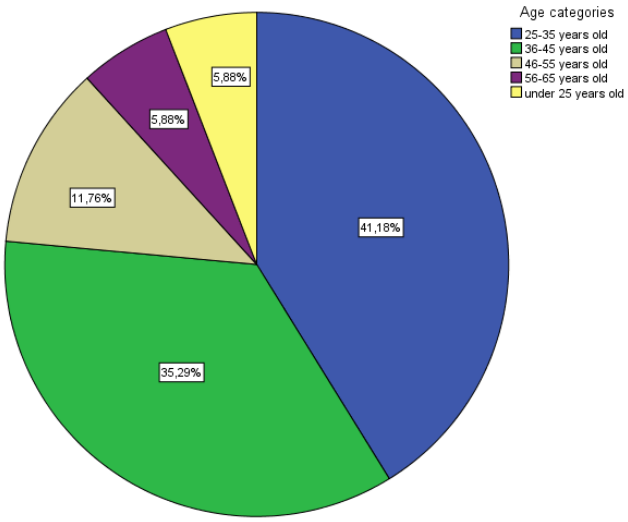


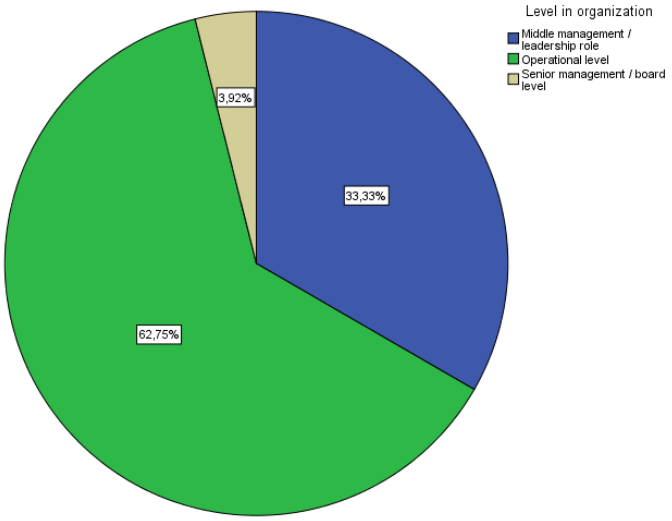


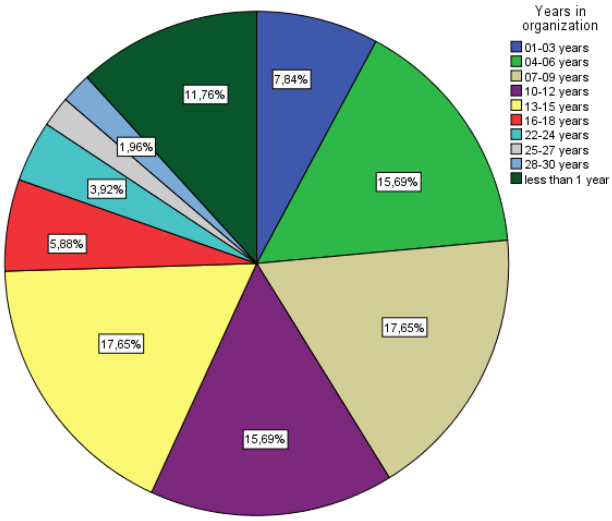
27 Appendix E (Demographics of research context 4)

Below the demographics are shown including a legend per pie diagram.



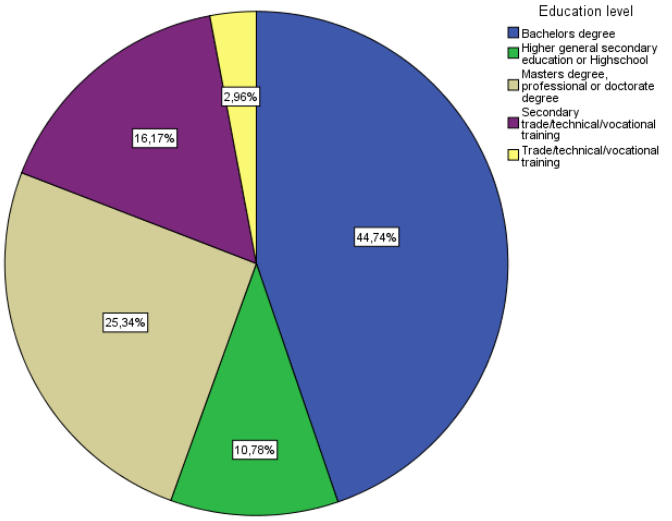


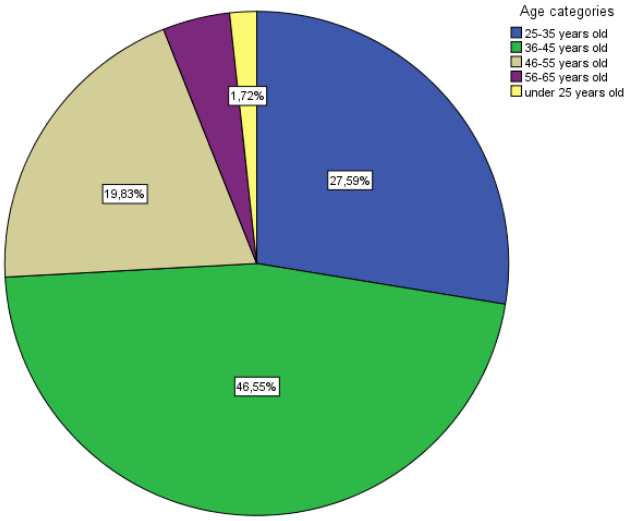


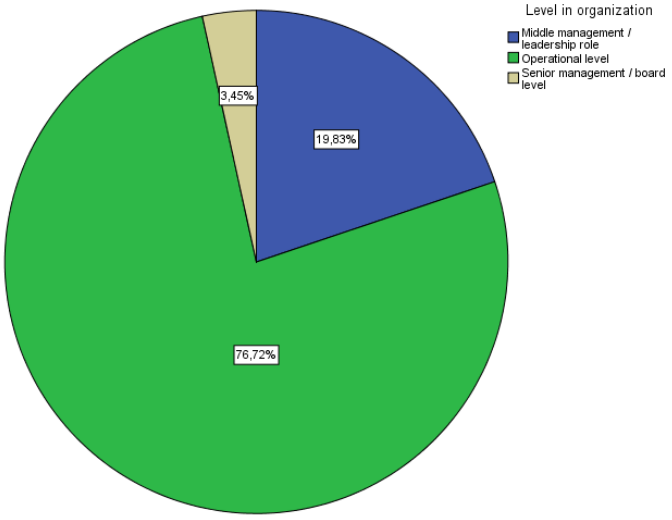


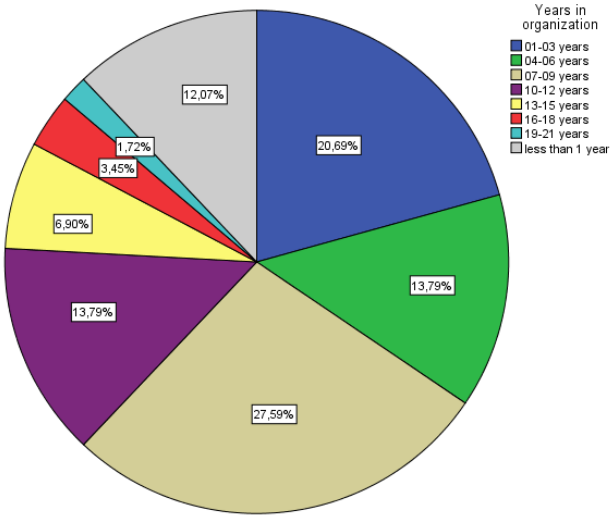
28 Appendix F (Demographics of research context 5)

Below the demographics are shown including a legend per pie diagram.









29 Appendix G (Additional findings)

Besides the findings already reported in chapter 18, some additional findings are worth mentioning within this appendix.

29.1 Delta on obvious / sure

From the answers on the survey a delta is seen between the questions:

- **It is obvious that** the majority of employees comply with the organization information systems security policies to help protect organization's information systems
- **I am sure that** other employees comply with the organization information systems security policies

In all measured contexts a delta is seen where in general the respondents agree on the fact that it is obvious to comply. Although respondents find it obvious, they doubt on the actual behaviors of their peers and have a neutral response on the 'I am sure…' question.

For context 3 the delta is less steep in comparison with the other contexts, which might induce more faith between the peers of that organization, which is a positive finding for context 3.

This effect is shown in Figure 44.

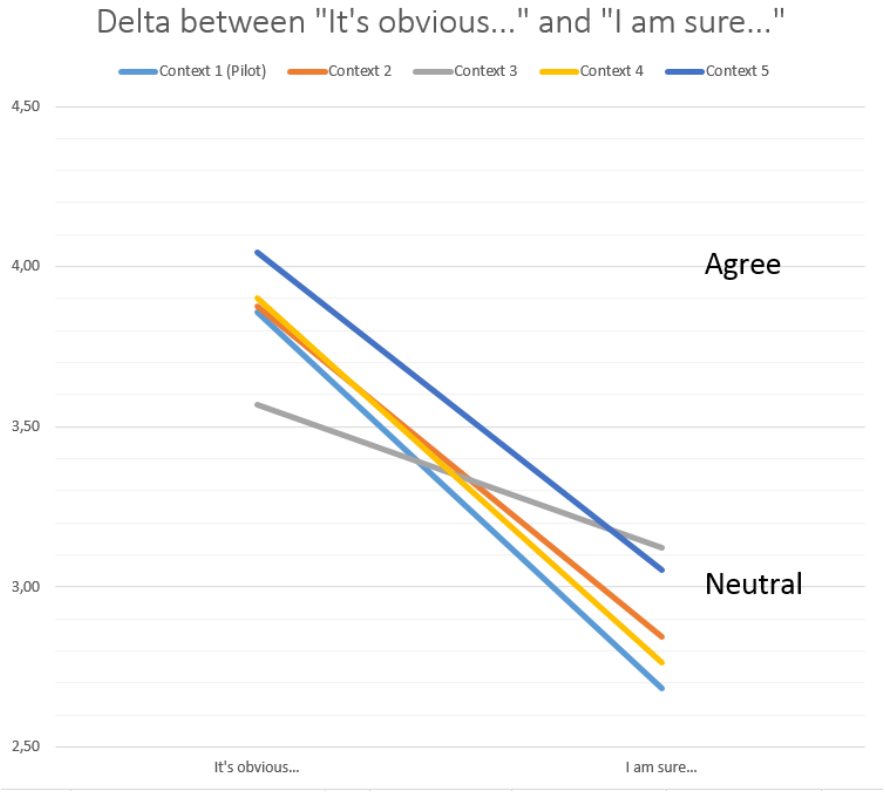


Figure 44 Delta obvious/sure

29.2 Delta on internal / external threat

From the answers on the survey another delta is seen between the questions:

- 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**

In all measured contexts a delta is seen where in general the respondents agree on the fact that they feel the need to protect their organization's information from external threats. At the same time they respond neutral on the need to protect from use by others within their organization. Prior research suggests that a substantial proportion of security incidents originate from inside the organization (Stanton et al., 2005).

The delta confirms the traditional external viewpoint on threats but at the same time shows awareness on threats from inside the organization because the lowest mean value is still above neutral level for all contexts.

This effect is shown in Figure 45.

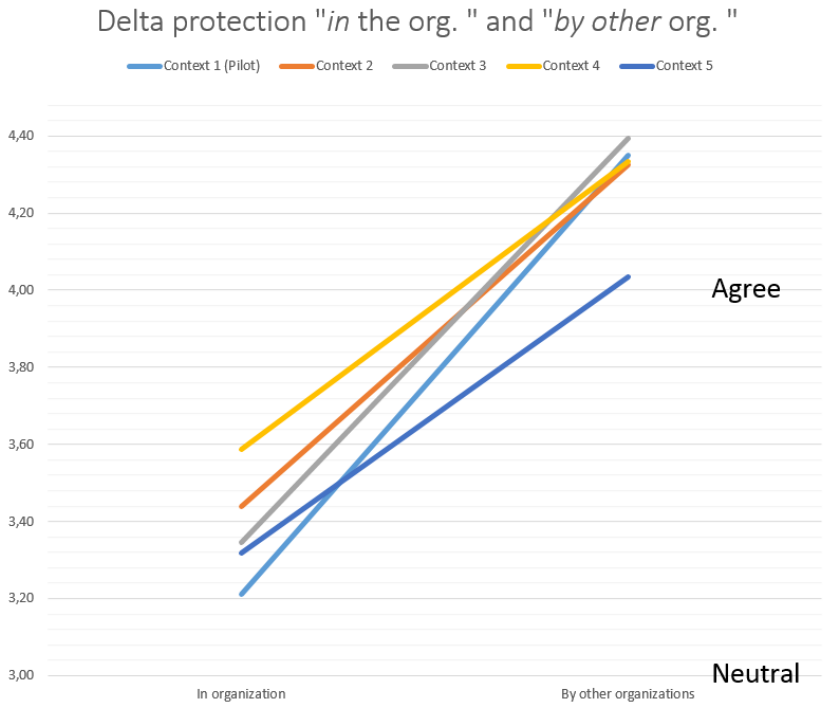


Figure 45 Delta on need to protect

29.3 Familiarity differs per organizational level

From the measurements on ISP status is concluded that besides influencing the motivational factors, familiarity to the ISP and finding the ISP applicable to the organization is found to be an important starting point in improving compliance to ISP (Albrechtsen, 2007).

Improving familiarity to the ISP differs from utilizing the motivational factors. The latter goes from the principle that the level of familiarity is a 'fact of the context' you have to deal with and despite that level, conditions can be shaped to improve compliance. Improving familiarity is the other way around and starts at the base that making end-users more familiar and show them the ISP is applicable, lets them further associate with the policy. This association is another way of improving compliance to ISP (Albrechtsen & Hovden, 2009).

The measurements confirm the expectation that management and board level are more familiar with the ISP because of their accountability and responsibility towards the ISP (Mears & Von Solms, 2007; Ponemon Institute, 2015).

This effect is shown in Figure 46.

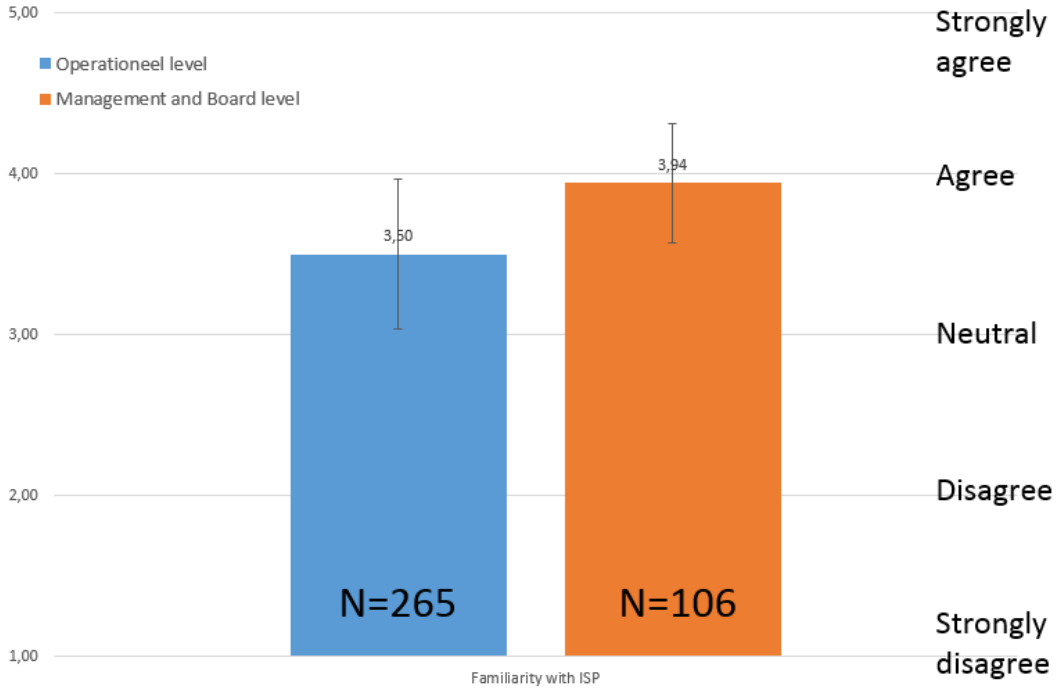


Figure 46 Familiarity differs per organizational level

29.4 Motivational synergy

Motivational synergy is the positive combination of intrinsic and extrinsic motivation (Amabile, 1993). Figure 47 recalls the two types of motivation factors. Emperical support shows that intrinsic motivation can interact constructively with other forms of motivation (Grant, 2008; Ryan & Deci, 2000a). The research of Amabile (1993) found that extrinsic motivation is most likely to combine synergistically with intrinsic motivation when the initial level of intrinsic motivation is high. As shown in Figure 48 and Table 42 the contexts 2 and 4 can provide from their position on the balance. At the same "certain types of extrinsic motivators will not add positively to intrinsic motivation, and will often detract from it. These non-synergistic extrinsic motivators are those that lead individuals to feel controlled or constrained by external forces" (Amabile, 1993). Especially for context 3 and 5, where the balance leans more to extrinsic, these controlling external forces deserve some additional attention.

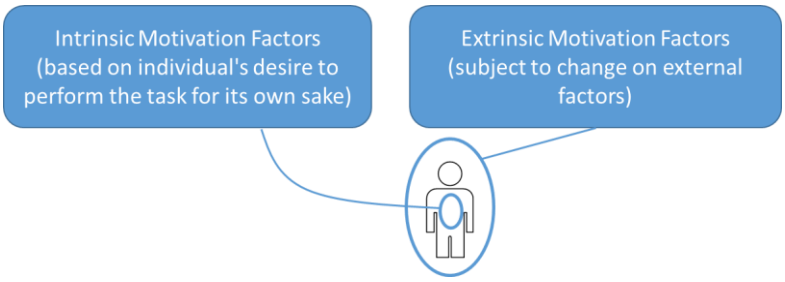


Figure 47 Intrinsic vs. Extrinsic motivation

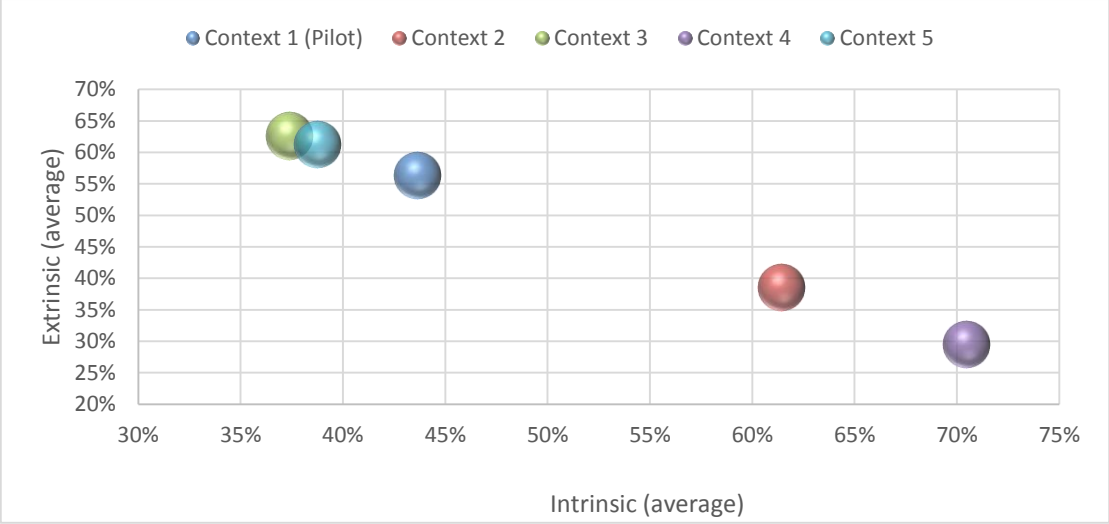


Figure 48 Balance between Intrinsic and Extrinsic

		Context 1 (Pilot)	Context 2	Context 3	Context 4	Context 5
Intrinsic	Sense of ownership Effect of actions	44%	61%	37%	70%	39%
Extrinsic	Data Governance Information Classification Normative Beliefs Peer Behavior	56%	39%	63%	30%	61%

Table 42 Balance between Intrinsic and Extrinsic

30 Appendix H (Article)

The article on this thesis is attached after this page…

PROMOTE END-USERS COMPLIANCE TO THE INFORMATION SECURITY POLICY: A COMPARISON OF MOTIVATIONAL FACTORS BETWEEN FIVE ORGANIZATIONAL CONTEXTS

Peter Straver
HU University of Applied Sciences Utrecht
Student ID: 1636125, peter.straver@student.hu.nl

ABSTRACT
Business information, held within information systems, is critical for most organizations. To protect these critical information assets, security controls should be deployed which might come as a hindrance for the end-users, on top of other demands in their work. The Information Security Policies (ISP) give direction to their behavior. Conditions can be shaped by organizations likely to promote so-called motivational factors influencing the end-users intentions to perform the desired behavior of compliance to the ISP in order to protect these information assets.

In total, six motivational factors, applicable to intentions on compliance, are found during research and are measured within five organizational contexts. From the measurements and analysis is learned, that the degree to which these factors relate differs per factor and per context. Two of these factors were found to always relate in such degree to compliance intentions that even without measuring the degree for a particular organization, applying these factors can be very effective for any organization or context. The other four factors have shown to be effective within particular context(s) meaning measurement of the context, with the instrument delivered from this research, is needed before utilizing these factors within an organization to optimize the effect of efforts.

1. Introduction

This article follows on my thesis research in the field of information security in culmination of the Master of Informatics in the field of Information Management and reports conclusions on a comparison of six so-called motivational factors between five organizational contexts.

Business information plays an important role for most organizations (Ifinedo, 2014). 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, & Anthony, 2009; Kritzinger & Smith, 2008).

"Many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security." (Bulgurcu, Cavusoglu, & Benbasat, 2010). Ponemon Institute (2014) found in their year 2014 research on the cost of data breaches at 314 organizations that 30% of the root causes for data breaches concerned employees or contractors abuse. A serious threat to the organization is seen to be formed by employees, not adhering to the information security policies (Siponen, Mahmood, & Pahnila, 2009). Hindrance caused by security practices is one of the reasons employees dislike such practices (Herath & Rao, 2009a).

It is recognized that one approach for making information security effective within organizations is to promote good end-user behaviors and constrain bad end-user behaviors (Stanton, Stam, Mastrangelo, & Jolton, 2005). To give direction to these behaviors a necessary foundation is found in ISP to define the concepts of information security (Knapp et al., 2009; Mears & Von Solms, 2007). A beneficial approach to compliance requires organizations to focus on their own non-malicious employees' intentions and behaviors towards compliance to the ISP (Ifinedo, 2014).

"A central factor in the theory of planned behavior (TPB) is the individual's intention to perform a given behavior. Intentions are assumed to capture the motivational factors that influence a behavior; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behavior. As a general rule, the stronger the intention to engage in a behavior, the more likely should be its performance." (Ajzen, 1991)

Therefore, within a context of information security, conditions can be shaped by organizations likely to promote motivational factors influencing the individual's intentions to perform desired behavior (Ajzen, 1991; Ifinedo, 2014; Ryan & Deci, 2000; Stanton et al., 2005; Weber, Otto, & Osterle, 2009). In the end, the individual's intentions should lead to the desired behavior of compliance to the ISP which in turn leads to an increased level of protection of the organization's information and technology resources (Bulgurcu et al., 2010).

Several motivational factors can be used in order to influence the intentions of end-users to comply with their applicable ISP. The problem is: **"Which to use?".** The conducted research gives answer to the question: **What motivational factors relate, in which degree, to intentions on compliance and how could these insights be utilized to promote end-users compliance to ISP 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.

The research developed and delivered an research instrument, ready to use in practice, in order to measure an organizational context on the effects of the six motivational factors recognized. These applicable motivational factors are determined from literature, judged and refined by Subject Matter Experts. A survey is conducted within five contexts, within five different sectors. From the statistical analysis, findings are reported and conclusions on the hypothesis are drawn.

This article is structured in four sections. In Section 2, a framework is constructed leading to a final conceptual model and stated hypotheses. In Section 3 the framework is operationalized by developing a survey instrument. In Section 4 the instrument is applied within five organizational contexts. The article concludes with section 5 summarizing the findings.

2. Framework Construction

End-user behavior can be influenced in different ways (Stanton et al., 2005). Different research areas with a focus on influencing malicious and/or non-malicious behavior have been researched in the past years, for which an overview is presented in Table 1 below.

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

Table 1 Overview of literature

From literature review and two subject matter expert sessions is learned that several factors surrounding compliance to such ISP have been researched in relation to policy compliance, for example in the area of deterrence (Straub, 1990), fear (Johnston & Warkentin, 2010) and neutralization (Siponen & Vance, 2010). Two factors (**Social Pressures** and **Effect of actions**) are adopted in this research' model from the already validated model of Herath & Rao (2009b). Two additional factors where less research on the relationship of these factors to policy compliance can be found in current literature are recognized, being:

- **Information Security Governance** (recognized in relation to compliance by several publications (Andersen, 2001; NEN-ISO-27002, 2013; Posthumus & Von Solms, 2004; Von Solms, 2006; Veiga & 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 & Barki, 2010))

Although these factors are recognized in relation to compliance to ISP, no relevant research has been found where Information Security Governance or Sense of ownership are researched as a motivation factor on compliance to ISP.

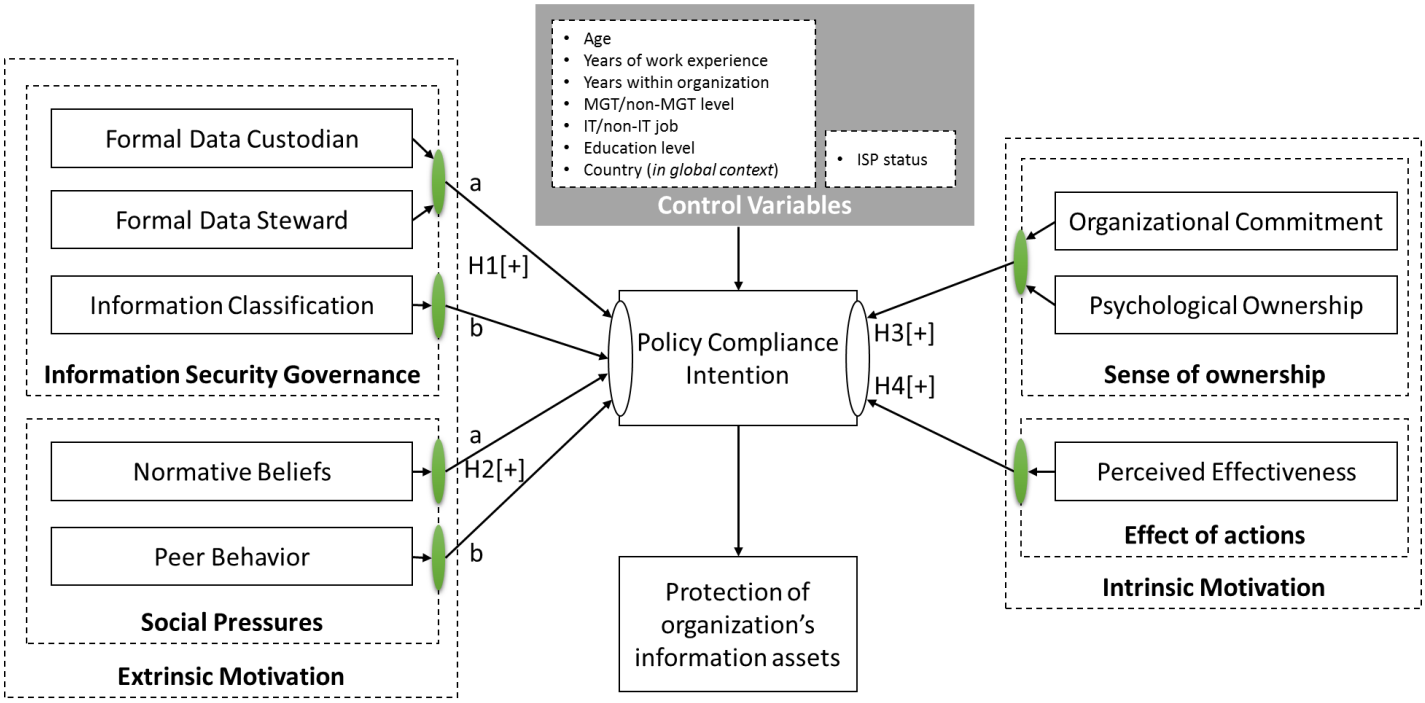


Figure 1 Conceptual model

The conceptual model shown in Figure 1 contains one dependent variable (Policy Compliance Intention(PCI)), being influenced by six main motivational factors containing a total of 8 elements forming the independent variables. To control whether other variables have an influence on PCI, some control variables are in the model as well. The model shows the relationships to be researched within the specific context of a given organization.

It is expected to find positive influences on all hypothesized relationships (H1 till H4) in the model:

H1(positive)	Information Security Governance positively influences PCI
a)	by elements of data governance measured separately
b)	by element information classification measured separately
H2(positive)	Social Pressures positively influences PCI
a)	by element of normative beliefs measured separately
b)	by element of peer behavior measured separately
H3(positive)	Sense of ownership positively influences PCI
H4(positive)	Effect of actions positively influences PCI

In Section 3 the framework is operationalized by developing a survey instrument.

3. Framework Operationalization

In order to operationalize the model, survey questions are designed 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 pilot survey is conducted within a pilot context after which the results are analyzed in order to refine the research instrument where applicable.

With the conceptual model as a starting point, all factors have a mapping to at least two sources of literature. To get more feeling on the context and status of the policy, several questions are included measuring status and perception around ISP as shown in Table 2.

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

Table 2 Survey questions and variables

Statistical Package for the Social Sciences (SPSS) software is used to analyze the conducted 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 (with a Greek symbol of α) 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 on 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).

In the next section the framework is validated by conducting the survey instrument.

4. Framework Validation

After consulting over 25 organizations for participation, four organizations responded in an enthusiastic manner and were able to get the needed mandate for sending out the distribution email for participation in the survey within the timeframe of the research. These are:

Context 1: Company in the business of ICT Security (conducted in pilot)
Context 2: Healthcare Consultancy and Insurance company
Context 3: Marketing Technology company
Context 4: Retail company
Context 5: Financial Services company

Each context was given the same amount of time to fulfill the survey. Table 3 show the status on the closing date of the last request.

	Context 2	Context 3	Context 4	Context 5	Total-4 contexts
Requested	403	180	110	300	Sum of 993
Started	179	103	72	163	Sum of 517
Responses	123	81	51	116	**Sum of 371**
Response rate	30,52%	45,00%	46,36%	38,67%	**Average: 40,14%**

Table 3 Response rate on final surveys

These results provide the needed data to be analyzed. First, data is **imported** and **recoded** and textual variables are turned into numerical values within the data file 'total-4' which form a dataset to first statistically analyze the final model and research instrument and provide insights in the total of measured contexts using the 371 responses. The outcomes of the **factor analysis** shown in Table 4 (first column) provide evidence on the items in the survey belonging together per factor/element and measure a single construct per factor/element.

The **reliability analysis** on the factors as seen in the factor analysis took place leading to the results shown in Table 4.

Factor / element	Context total-4	Comment
Policy Compliance Intention **INT1 INT2 INT3**	α = 0,827	**Reliable**
Normative Beliefs **NORM1 NORM2 NORM3 NORM4 NORM5**	α = 0,892	**Reliable**
Effect of actions **EFF1 EFF2**	α = 0,878	**Reliable**
Peer Behavior **PEER1 PEER2**	α = 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**

Table 4 Reliability analysis for total of 4 contexts

For the 'total-4' 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 total-4 model.

Analysis of the total-4 dataset shows an averaged image of the paths for all four contexts as shown in Figure 2.

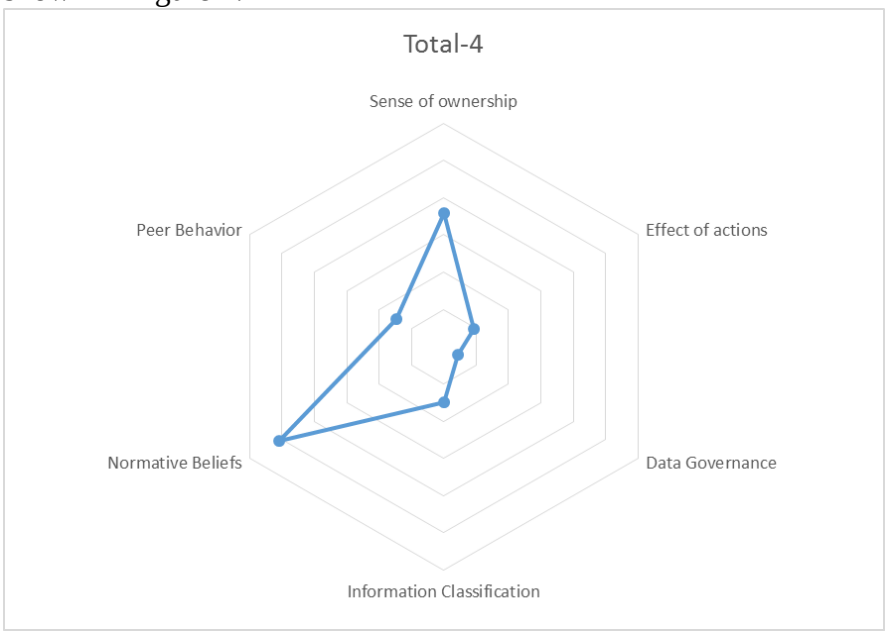


Figure 2 Path coefficients for total-4

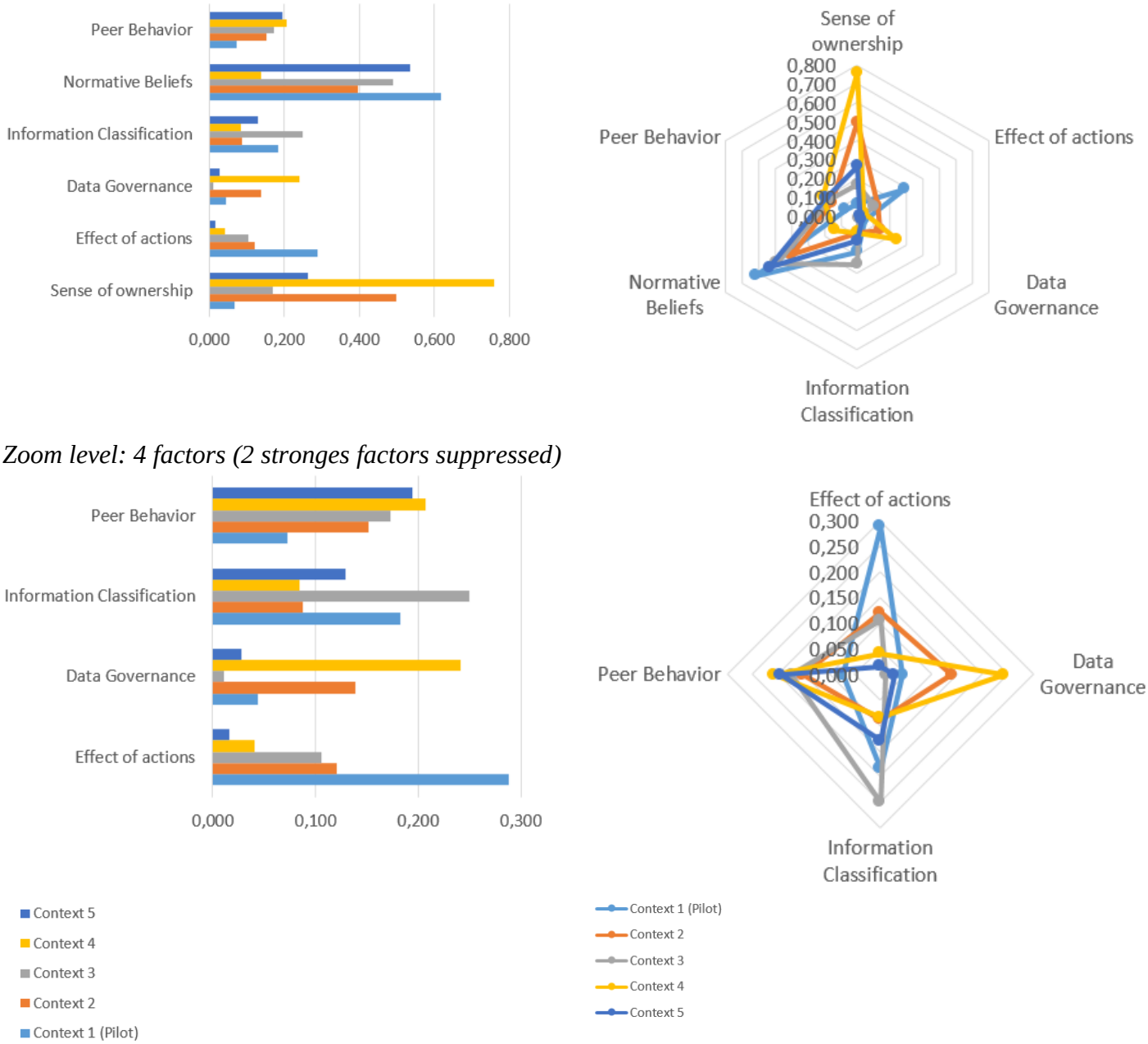
Total-4	***R2=***	***40,91%***
Sense of ownership	β =	0,358
Effect of actions	β =	0,092
Data Governance	β =	0,044
Information Classification	β =	0,151
Normative Beliefs	β =	0,509
Peer Behavior	β =	0,146

Table 5 Path coefficients for total-4

The coefficients values are summarized in Table 5.

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.

Zoom level: 6 factors



Zoom level: 4 factors (2 stronges factors suppressed)

Figure 3 Comparison of contexts

These insights lead to the main finding of the research: There lies a certain value in the generalized view on the motivational factors, but the motivational factors should be measured per context if an organization needs targeted advice on their organization specific security program.

In the next section the conclusions from research are summarized.

5. Conclusions and further research

As hypothesized, in general, positive influences on all recognized relationships are found in the research findings as shown in Table 6:

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

Table 6 Results on hypothesis

From the research findings the following conclusion are drawn:
Conclusion 1) In general, "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 the conditions to shape should have its 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. Normative beliefs are based on the belief as to whether or not a significant person wants the end-user to perform the expected behavior (Bulgurcu et al., 2010; Herath & Rao, 2009b; Ifinedo, 2014).

Conclusion 2) In general, "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 the conditions to shape should have its focus on empowering and allowing end-users to exercise a certain level of control over important aspects of their work arrangements. Aspects like job satisfaction and self-esteem improve sense of ownership (Avey, Avolio, Crossley, & Luthans, 2009; Van Dyne & Pierce, 2004; Mayhew, Ashkanasy, Bramble, & Gardner, 2007; Spears & Barki, 2010).

Summarized: **Shaping conditions around "normative beliefs" and "sense of ownership" always provides a positive influence to compliance, despite the context.**

Conclusion 3) From the findings of the research is further concluded that the four other motivational factors should first be measured within the specific organization context to determine their relevance to that context. Measurements show that some of these factors are missing any relevance for a specific context but do show significant relevance for another 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 these insights in practice follow for each factor:

- Effect of actions, as an intrinsic motivational factor, can be utilized in practice if conditions to shape by the specific organization have focus 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 & Rao, 2009b; Olckers, 2013).

- Data governance, as an extrinsic motivational factor, can be utilized in practice if conditions to shape have focus 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 & Chang, 2007; Lee & Strong, 2003; NEN-ISO-27002, 2013; Weber et al., 2009).

- Information Classification, as an extrinsic motivational factor, can be utilized in practice if conditions to shape have focus 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. Applying includes 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 & Hale, 2009; Puhakainen & Siponen, 2010; Veiga & Eloff, 2007).

- Peer behavior, as an extrinsic motivational factor, can be utilized in practice if conditions to shape have focus 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, & Kallgren, 1990). End-users seeing their co-workers routinely follow ISP are likely to carry out similar behaviors (Cheng, Li, Li, Holm, & Zhai, 2013; Cialdini et al., 1990; Fishbein & Ajzen, 1975; Herath & Rao, 2009a, 2009b).

To further enhance the recommendations more insights and knowledge on the motivational factors could be gained in case the instrument is applied to more contexts within the same segment / field of work in future research. Such research could provide further insights on the specific motivational factors and their relevance within a segment. There's a possibility these insights help shaping conditions for specific segments leaving out the effort of measuring a specific context in advance of a campaign or security program.

REFERENCES

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

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*.

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.

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.

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

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.

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.

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.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security*, *27*, 224–231.

Lee, Y. W., & Strong, D. M. (2003). Knowing-Why About Data Processes and Data Quality. *Journal of Management Information Systems*, *20*(3), 13–39.

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*.

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.

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., 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.