# Interpreting Information Security Policy Outcomes: A Frames of Reference Perspective

Marko Niemimaa
TUCS - Turku Centre for Computer Science
University of Turku, Turku School of Economics
marko.niemimaa@utu.fi

Anna Elina Laaksonen
Tampere University of Technology
anna.laaksonen@tut.fi

PhD Dan Harnesk
Luleå University of Technology
dan.harnesk@ltu.se

## Abstract

*A major concern for IS managers is that information security policies seldom produce expected outcomes. Previously, scholars have studied motivations underlying non-conformance to policies and proposed approaches for motivating employees. However, the socio-cognitive aspects that shape employees' perceptions of the policies and implications for policy outcomes have received modest attention. This study draws on socio-cognitive concept of frames and on literature on information security policies to suggest a theoretical and analytical concept of Information Security Policy Frames of Reference (ISPFOR). The concept provides a sensitizing device to interpret how the frames influence organizational groups' perceptions of policies and the implications of the perceptions on policy outcomes. Three frame categories were uncovered through an interpretive case study at large multinational internet service provider. Findings suggest frames shape perceptions of policies and provide an explanation for unanticipated policy outcomes. Implications for research and practice are discussed.*

## 1. Introduction

According to a recent industry survey, over 90% of large enterprises have implemented information security policies (hereafter InfoSec policies) [23]. However, despite the recognized significance of InfoSec policies and the fact that organizations devote resources to formulate and implement them, the policies as Information Security Policy Frames of Reference (ISPFOR). Borrowing the concept of congruence from Orlikowski and Gash [21], we argue that ISPFOR congruence is the extent of similarities in policies seldom produce the intended outcomes [14]. In efforts to understand this concern, scholars have studied motivations underlying non-conformance to policies (e.g., [10], [2], [26]) and proposed diverse approaches for motivating employees towards policy compliant behavior (see [24] for review). Such studies acknowledge many different actors influence the policy outcome.

Any approach to information security management needs to integrate the variety of interpretations that organizational members have about the information security practices [28]. Indeed, Hsu (2009) [11] points out that "having an appropriate understanding on how different groups perceive IS security can strengthen the design and institutionalization of security management practices." (p. 149). Therefore, an understanding of how groups perceive InfoSec policies is central in helping IS managers to understand the unanticipated policy outcomes and in providing them with approaches to solve such outcomes. Unfortunately, perceptions have largely remained unexplored in the literature. In particular, the involved socio-cognitive aspects have not been studied. To address this concern, this paper draws attention to the organizational groups' perceptions of InfoSec policies by discussing how socio-cognitive structures shape groups' perception and explain adversities and unanticipated policy outcomes.

We draw on the widely used theory on frames of reference (hereafter frames) [31] to analyze the employee perceptions of InfoSec policies. Frames are organized knowledge that represent an information domain [31] and shape how individuals perceive and make sense of different phenomena. We call the frame that represents and shapes the perceptions of InfoSec the category content among organizational groups. In other words, when the ISPFOR category content sharessimilarities across organizational groups, those parts of ISPFORs approach congruence. As follows,

1530-1605/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2013.282

incongruence is the extent of differences in the category content among organizational groups. We use interpretive case study [15] [32], building on semi-structed interviews and on hermeneutic interpretation as the research methods. Our results suggest the frames can largely explain the adversities and unexpected policy outcomes experienced at the case organization.

The paper is structured as follows. First we develop a conceptual framework for this study by positioning frames to InfoSec policy research. Second, the chosen research method and its data collection and analysis strategy are explained. Third, we discuss the findings and the implication for researchers and for practitioners. Finally, we conclude by summarizing the most central findings.

## 2. Informing theoretical elements

### 2.1. Information security policies

InfoSec policies are a set of documents that define the strategic direction for information security in an organization [13] and give instructions for employees as to what they are expected to do when they interact with organization's information systems [34]. There is a growing agreement among researchers and practitioners that InfoSec policies are the foundation of information security in an organization (e.g., [1], [25], [6]). The implementation of the InfoSec policies is one of the most important information security controls [12] and an integrated part of information security governance [29] and strategic information security [18]. Indeed, the InfoSec policies should be directly linked to organization's objectives and strategic planning [7]. The purpose of InfoSec policies is to influence employees' perceptions of information security towards a shared understanding throughout the organization [22] and to guide them towards information security aware behavior [34]. Despite the recognized significance of InfoSec policies, they seldom produce the intended outcomes [14].

InfoSec policies should be implemented by disseminating them throughout the organization and by providing employees adequate training [12]. In order to achieve the anticipated benefits, InfoSec policies must be used appropriately by all employees [30] and translated into actions [33]. In practice, there is often a conflict in espoused theory and theory-in-use [5]. Despite the recognized significance of InfoSec policies and of the implementation and use issues, only limited scholarly contributions exists. In particular, employees' perceptions of InfoSec policies have been left for little attention. Such studies are needed [27]. Understanding these perceptions is imperative as, in the long run, it is the employees who determine the success or failure of the InfoSec policies [12].

### 2.2. Theory of frames of reference

Frames have significant influence on how individuals act [21] [17]. The use of frames in information processing may encourage stereotypic thinking, fill data gaps with information that fits in to the existing frame, discourage questioning the existing, already formed knowledge structures and inhibit creative problem solving [31]. Frames ensure that information that drastically challenges the validity of frames rarely occurs, instead, as the frames direct search for and acquisition of information, it is more likely that information uncovered will only reinforce already existing frames [9]. Within information security research, Hsu (2009) [11] has used frames of reference to denote organizational members' expectations and knowledge of and assumptions about the implementation of an international information security standard and studied how frames shaped organizational members' actions.

As organized knowledge frames consist of structure and content. Structure refers to categories of knowledge and content to specific knowledge within a specific category [21]. Frames are always situated in the context of particular time and space and thus should be analyzed *in situ* rather than be assumed *a priori* (ibid.). Although frames are formed at individual level, the frames can become shared on a group, organization or even industry levels [31]. Frames can become shared through the course of socialization [11], or through shared experiences and shared exposure to social cues about other employees' reality [9]. These group-level, shared frames function in a similar manner as individual knowledge structures, despite the cognition occurs at individual level [3]. As frames are formed through individual experiences and shared through, for example socialization, it is likely that different organizational groups form differing frames concerning the same phenomenon. Incongruent frames [21], may have substantive organizational consequences.

## 3. Information Security Policy Frames of Reference - ISPFOR

InfoSec policies are formulated, implemented and used by employees. During these processes, employees form perceptions of these policies and form a frame that concerns InfoSec policies consisting of the understandings, assumptions and expectations they become to have around the InfoSec policies. We call

this frame 'Information Security Policy Frame of Reference' (ISPFOR). It provides a sensitizing device for this study to interpret organizational groups' perceptions of InfoSec policies and the implications on policy outcomes.

The content of ISPFOR, structured into categories, is the set of employee's understandings of, assumptions about, and expectations of InfoSec policies. As frames are situated in time and space [21], her experiences around InfoSec policies can evolve and the structure and content change accordingly. This contextual dimension is important as InfoSec policies only have a meaning and function the employees give them in a specific context; the meaning of InfoSec policies does not reside in the documents themselves. Both explicit cues such as documents and organization's information security awareness campaigns and implicit cues such as those embedded in organizational culture and interaction between people can act as inputs for the formation of ISPFOR. In other words, ISPFOR emerges from and is transformed by interactions between employees, documents and context. Therefore, ISPFOR does not only consider the documents *per se* but contains knowledge about all experiences employee has related to the InfoSec policies, their use and their contextual consequences. When employees, for example, share similar organizational roles in regard to organization's InfoSec policies or work closely together in questions related to policies, they are likely to share similar experiences and receive more social cues from each other, gradually shaping their ISPFORs, making them more similar and eventually shared.

In an organizational context, ISPFOR may have substantive consequences. Many of the issues associated with InfoSec policies; employee resistance, skepticism, non-compliance [12]; are largely similar to ones information systems (IS) research has identified in relation to technology and argued that many of the issues originate from frame incongruence [11]. Building on this research, we suggest that incongruence in the organizational groups' ISPFORs is likely to influence InfoSec policy implementation and use (Figure 1).

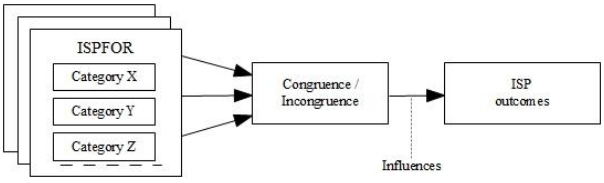


**Figure 1: Conceptual framework: ISPFOR influences InfoSec policy outcomes**

In this study the framework was used in two ways: (1) as an initial guide to design the data collection; and (2) as a part of an iterative process of data collection and analysis [32], functioning as a sensitizing device to interpret the perceptions of InfoSec policies and the implications of the perceptions on policy outcomes.

## 4. Research approach

This interpretive research builds on the principles brought forward by Klein and Myers (1999) [15] for conducting interpretive research. As interpretive researchers we accept that the data available to us are subjective meanings of informants and we attempt to understand these meanings from their perspective [20][15][32]. Our conceptual framework guided the design of the case study and data collection and formed a part of the iterative process of data collection and analysis. As understanding can be only gained through a cyclic, iterative process of going between the parts and the whole, it guided our data analysis drawing on our conceptual framework and resulting into findings of this study, creating a dialogical process between data and the theory [15].

### 4.1. Data collection and analysis

Nineteen semi-structured interviews [16], lasting approximately one hour, were conducted in accordance with our interview guide. The interview guide covered three main areas: (1) information security policies and their relation to interviewee's work and responsibilities; (2) the value of information security policies for the interviewee; and (3) the future of information security policies. Reflecting the hermeneutic circle [15], through social interaction between the informant and us, a whole of shared understanding emerged during each interview. Individual field notes were collected. All interviews were recorded and transcribed shortly after the interview. To confirm our emerged understanding of the informants' perceptions, a summary of our interpretations was discussed with the informants. As a result, the data we collected were created in part and parcel with our informants (ibid.). The data we collected through interviews were only identified by their respective group and not individually, providing a degree of anonymity. Additional data sources were used to improve the understanding of the context and provided us with factual information when constructing the social and historical context (ibid.) of the study.

The choice of the informants in the study was guided by conceptual questions, rather than representativeness [19]. Keeping in mind the conceptual framework of the study, informants were selected so that they represent four organizational

groups and so that they could be assumed to have experiences from their organization's InfoSec policies. The number of informants was decided as we proceeded with the data collection and was driven by two conditions [16]: (1) the aim of the study was not to make statistical generalizations, but to interpret informants' perceptions of InfoSec policies, thus a too extensive number of interviews would have made careful interpretation practically impossible; and (2) interview as many persons as is needed to arrive to an understanding of the phenomenon.

We identified four distinct organizational groups whose perceptions were studied. Three of the selected four groups emerged through conversations with organization's information security professionals and reflected their concern over the perceived unexpected policy outcomes amongst groups that had significant importance for the organization's information security. The groups represent three different hierarchical levels of the organization:

*IT Solution Managers (ISM)* were responsible for coordinating IT system maintenance and development. They gathered requirements for IT system changes, ran negotiations with IT system vendors and oversaw production environments, but did not do actual system configurations; *IT Solution Owners (ISO)* were responsible for a team of IT Solution Managers. As positioned between the IT Solution Managers and Senior Managers, they were involved in decision making in regard to systems maintenance and development and tried to 'get things done'; and *Senior Managers*.

Later on, as our understanding grew, a fourth group, Information Security Professionals was included as including it was seen to enrich our study. As the members of the three previously selected groups were located in either Finland or Sweden, the group of Information Security Professionals was also selected so that members were located in Finland and Sweden.

Hermeneutic understanding of the interplay between the parts and the whole together with the iterative nature of the analysis drawing on the conceptual framework of the study, during and after data collection, and frequent discussions between the researchers were central to our data analysis. Coding, pattern coding, and data visualization in a matrix were techniques used to analyze the data [19]. As soon as possible after each interview, no later than three days, interview transcript was examined for statements that reflected informant's understandings of, assumptions about, or expectations of InfoSec policies and coded accordingly (Table 1).

**Table 1: Coding examples**

| *Expression* | *Code* | *Interpretation* |
|---|---|---|
| *I think they [InfoSec policies] are in most case incomprehensible. It's too much, it's like close to 100 pages.* | Understanding | The statement reflects informant's way of understanding the InfoSec policies as incomprehensible, complemented with the description of 'why' those were perceived incomprehensible. |
| *The interpretation of it [InfoSec policies] is left for the system specialist or to the IT Solution Managers and those interpretations can be sometimes different from the same thing.* | Assumption | The statement reflects uncertainty whether there really are differing interpretations. The informant is assuming that what requires interpretation for him requires interpretation for others as well. |
| *A very good type of instruction [InfoSec policy] is just related to something like password form, that password must be this long, cannot be longer than this, and must contain these characters.* | Expectation | The statement reflects informant's expectation of the InfoSec policy content style through a concrete example. |

Pattern coding was then used to examine the coded data to find categories for each informant (Table 2).

**Table 2: Emerging preliminary categories**

| *Understandings, assumptions, expectations* | *Pattern* | *Interpretation* |
|---|---|---|
| *No... it just has to be done. All work can't be joy all the time, I mean... somethings just has to be done.* | Motivation to comply | The statement reflects informant's motivation for complying with the ISPs. |
| *I know information is safe, it goes my way, it doesn't flow all over the place, it doesn't go where it shouldn't go... I mean we need to have very extremely good control of our systems, they are in good shape and they do what they are supposed to do. So... yea... vital* | Value of InfoSec policies | The statement reflects the InfoSec policies value for the informant. |

Within each studied group, categories for each informant were compared to other informants' dittos to uncover categories shared across all group members. Table 2 shows examples of preliminary categories that emerged during the analysis. Data from each informant within a group was then reexamined, to validate whether the newly emerged categories would represent each informant's coded data and our interpretations that had emerged during the course of the interviews. Finally, validated categories from all groups were compared for more abstract analytical categories that would be shared across the groups. The data were reexamined using the proposed analytical categories. This cyclic, iterative process led to three analytical categories that were proposed to represent the categories of the informants' ISPFORs. Finally, we drew on our conceptual framework to analyze frame incongruence among the studied groups. Here, different matrices were used to visualize the data and content in each analytical category was compared and contrasted across the four organizational groups.

## 5. Case study: Beta

This case study is concerned with four organizational groups' perceptions of the organization's InfoSec policies in one large, multinational, internet and telecommunications service provider. The description of the social and historical context provides a view how the current situation has emerged and how the organization has implemented the current InfoSec policies [15].

Beta (a pseudonym) is a publicly traded company, which operates in 20 markets, in Nordics, Baltic countries and in the emerging markets of Eurasia, employing approximately 30 000 persons. It provides network access and telecommunication services both to business and private customers. Due to the type of data processed and stored and services provided, Beta's business operations are highly regulated. Security is seen as part of quality, which is one of Beta's core values. Information security is defined as 'the sum of all protective measures to insure that correct information is made available when needed to people authorized by Beta only'. Beta has a centralized security organization, responsible for overseeing security, and a set of supporting country organizations.

## 5.1. Information security approach at Beta

Beta's motivation to create InfoSec policies (i.e., top-level policy and instructions) is 'to steer information security'. Policies are a result of an evolutionary process, currently maintained by Beta's Information Security Professionals. Guidance has been sought from international standards and best practices, by conducting informal benchmarking against competitors and by analyzing external threats. The InfoSec policies are disseminated through a dedicated section on Beta's intranet where access to the documents is complicated and the documents are poorly indexed. E-mail notifications are sent to some employees after larger changes. While compliance is mandated by the top level document, no systematic measures have been taken to direct employee behavior. The security state of key IT systems is, however, reviewed periodically through checklists that document a range of high level systems security requirements. The checklists refer to InfoSec policy documents for more details. These periodic controls are referred as 'periodic IT system controls'. After each periodic IT system control, the state of the system is reported using traffic light colors (green, yellow, red) to signal the outcome of the controls and to provide strategic metrics for Beta's management.

## 5.2. The emergence of incongruence

The four studied groups shared an understanding of why Beta formulated and implemented InfoSec policies - to protect Beta and its information. Their expectations for a means to an end, however, differed: ISMs expected InfoSec policies to protect the organization and its information by defining requirements for IT systems and their configuration; ISOs by bringing unity to the organization, mainly by imposing IT system requirements for ISMs to implement; Senior Managers by stating clear responsibilities for employees; and Information Security Professionals by their mere existence. In addition to the shared understanding of organizational importance, the purpose of the InfoSec policies was viewed from role related perspectives that had resulted in ISPFOR incongruence.

Each groups' role in relation to InfoSec policies and their interaction with the policies had affected the content of their ISPFOR; the frame content differed between groups and partly even within each group. The differences in group members' frames can be attributed to the lack of close contact between the group members as, as argued, the ISPFORs become shared through the course of socialization. In particular, the ISMs that were located in physically distant offices and that rarely interacted with other ISMs had differing frame content from those ISMs who were in closer contact with each other. However, even in such cases the ISPFORs were largely similar. Their common role in regard to InfoSec policies seemed to shape their frame content through introducing similar experiences of the InfoSec policies. The periodic IT system controls, that formed a part of ISMs' role, engaged them into similar situations where they tried to read, interpret and apply InfoSec policies.

*Incongruence #1. Incongruence occurs as each group has its own unique background, responsibilities and concerns that affect their expectations of the InfoSec policies.*

## 5.3. Incongruence in InfoSec policy implementation practices

Using the InfoSec policies was a concern for ISMs, ISOs, and Information Security Professionals. They had formed an understanding of the InfoSec policies as overly long documents that needed interpretation before they could be applied into practice. Although ISMs and ISOs perceived that the current InfoSec policy documents should be complemented with more detailed guidelines, detailed guidelines were not expected to substitute constant and much needed support from Information Security Professionals. As one of the ISOs expressed her concern:

"Security department if I may call them so... they could be more active and be more out in... in among the system owners and... have more sort of follow ups and discussions with us. (ISO)"

Some of the ISMs and ISOs were frustrated as they had previously been guided back to the InfoSec policy documents when they had asked for support for applying the policies. Indeed, Information Security Professionals had a document centered approach to the InfoSec policies and requests for support were merely perceived to be a deficiency in the InfoSec policy documents and complementing them with more detailed guidelines was assumed to be in-line with ISMs' and ISOs' frames and an efficient way to satisfy the organization's needs.

"We have limited resources, if we think about our staff, then it's easier for us to produce documentation, easy to comprehend documentation, that we can then push to the business, advice them that the documentation is available on our intranet page and if they obey it everything is fine." (Information Security Professional)

Although previous research has suggested that document centered approach is one of the least effective information security measures [8], the approach was not actively questioned by the Information Security Professionals. Reflecting frames' tendency to encourage conventional thinking and inhibit novel problem solving, Information Security Professionals expected that a means for reducing the amount of requests for support was to be found from more specific, detailed documents as suggested by international standards and best practices, or by adopting supporting software solutions. They did not actively seek to improve the usability of the InfoSec policies through seeking to understand other groups' expectations of how the usability should be improved. ISMs and ISOs frames were incongruent with Information Security Professionals and this incongruence was apparent in ISMs' and ISOs' frustration and how ISMs and ISOs used the InfoSec policies.

Having InfoSec policies and information security visible in the organization was important for each of the groups. The groups' ISPFORs were, however, incongruent on what was seen to be sufficient visibility. Information Security Professionals, reflecting their document centered approach, appreciated Beta's intranet as a means to disseminate and educate employees about the InfoSec policies; the self-motivated employees should proactively go, read and adopt the information in the InfoSec policy documents. However, this approach was not appreciated by the ISMs or ISOs.

"We have some group IT policy or some page like that somewhere in our intranet, where we are apparently supposed to go by ourselves and check how these policies [InfoSec policies] have changed, always." (ISM)

Indeed, the intranet was seen by most, especially the ISOs, as a place where the InfoSec policies were lost, as if they were 'in a sea' as one the ISOs metaphorically expressed her concern. Accordingly, ISMs and ISOs, who shared similar view on the matter, assumed that sufficient visibility could be achieved through presentations, awareness campaigns, and through Information Security Professionals' participation to the day-to-day work of the employees. Indeed, as one of the ISMs expressed herself, the assumption was that Information Security Professionals are responsible of motivating the employees:

"Cause you see... that's how we're missing information from the security guys... they should keep everyone on track, make us burn for it!" (ISM)

*Incongruence #2. The ISPFOR incongruence is visible in misaligned expectations of the content and structure of InfoSec policy documents, available support for using the InforSec policies and the visibility of InfoSec policies and information security within the organization thereof.*

## 5.4. Incongruence in deploying InfoSec policies

Information Security Professionals assumed that InfoSec policy documents, when clear enough, are proactively used by employees to adopt compliant behavior on their own. Their ISPFOR had shaped their actions by encouraging conventional thinking; Information Security Professionals focused on producing the documentation and publishing it on the intranet. Nevertheless, Senior Managers, ISOs and ISMs assumed their normal work routines were in-line with the InfoSec policies. They expected that appropriate routines could be simply picked up from the environment as they had done in the past, thus InfoSec policy documents were left mostly untouched.

"We have gotten used to it so... it is like in the spinal cord that you don't really think about it, it is like self-evident. It is part of the work. I don't see it as a separate thing, it is just there with us" (ISM)

Their expectation of picking up routines by living in the organization was in-line with their expectations of InfoSec policy supporting activities: the policies were expected to be visible in their daily work, and indeed they expected policies to be brought to them. The evident ISPFOR incongruence had lead to colorful routines among different groups and even between individuals. At Beta, Information Security

Professionals' frames, that were reflected to the InfoSec policies, not only caused ISMs problems in comprehending the stated requirements, but also inefficient time use as ISMs had to spend time interpreting the InfoSec policy requirements.

It was not only the frames held by the Information Security Professionals that were reflected in the InfoSec policy document content, but rather the incongruence between the ISMs' and the Information Security Professionals' ISPFORs that had negatively impacted the ISMs' willingness to engage themselves in reading the InfoSec policy documents. For example, when ISMs and ISOs encountered novel or problematic situations, they rather resorted to their own common sense reasoning or to colleagues than searched for answers from the actual InfoSec policy documents. Resistance was reflected to their actions as the ISPFORs guided ISMs' and ISOs' information search and instead of resorting to InfoSec policy documents, the ISMs and the ISOs resorted to colleagues and other, less resisted, information sources.

*Incongruence #3. Incongruence influences groups' willingness to use InfoSec policies by shaping groups' perceptions of InfoSec policies as repugnant.*

To summarize, our analysis suggests that each group had formed a differing ISPFOR. Groups' role in relation to the InfoSec policies and their interaction with the InfoSec policies had shaped their perceptions. Incongruence among the four groups manifested itself in ISMs' and ISOs' frustration and resistance towards the InfoSec policies and had led Information Security Professionals to make choices in the InfoSec policy implementation that were assumed to be in-line with other groups' frames, but that, in fact, were not. Even though ISMs, ISOs, and Senior Managers preferred 'picking up' the correct routines from the environment rather than reading and interpreting the InfoSec policy documents, Information Security Professionals assumed the perceived issues can be addressed through complementing the current InfoSec policy documents with more detailed guidelines or with software solutions. The frame incongruence had led the groups to adopt colorful routines. However, as the more detailed guidelines and software solutions were more in-line with the Information Security Professionals' ISPFOR, they did not actively question their approach; they were guided by their already formed ISPFOR. Organizational groups' perceptions had consequences for the InfoSec policy implementation and use at Beta. Although Beta had dedicated resources to implement the InfoSec policies, our analysis suggest that, from frames of reference perspective, Beta's implementation efforts had gone partly in vain and resulted in unexpected policy outcomes.

# 6. Discussion

Despite the significant efforts organizations have made to implement InfoSec policies, the InfoSec policies have been found to be one of the least effective information security practices [8]. To this end, our case, Beta, presents a typical InfoSec policy implementation. While the organization was able to realize some benefits from the implemented InfoSec policies, the benefits were mostly overshadowed by the unexpected outcomes; the difference between the espoused theory and theory-in-use was apparent. Therefore, although the case we present was indeed a failure of InfoSec policy implementation, understanding the underlying reasons for the failure is beneficial.

Based on our interpretations, three ISPFOR categories were found to explain the experienced adversities and unanticipated policy outcomes by shaping the employees' perceptions. The analytical frame categories that emerged from the dialogical interplay between the data and theory [15], in which incongruence was apparent, were:

*Usefulness of InfoSec policies:* This category represents the part of groups' frame that refers to groups' understanding of why their organization formulates and implements InfoSec policies. It concerns their understandings of the value and importance of the InfoSec policies and assumptions about and expectations of what can be achieved by having the policies.

*Usability of InfoSec policies:* This category represents the part of groups' frame that refers to groups' understanding of how convenient it is to use InfoSec policies. It includes their understandings and expectations of the InfoSec policy document structure, content and content style as well as of the InfoSec policy implementation and supporting activities provided to complement the InfoSec policy documents.

*InfoSec policies in Use:* This category represents the part of groups' frame that refers to groups' understanding of how InfoSec policies are applied in their everyday work and in the organization. It concerns their understandings of when the InfoSec policy documents are used and understandings of and assumptions about InfoSec policy compliant behavior and its contextual consequences. It further concerns their assumptions about and expectations of their possibilities to influence the InfoSec policies.

Uncovering the frame categories afforded us to systematically analyze the groups' frames. Our sensitizing device, helped us to interpret the underlying mechanisms that shape the groups' perceptions and by doing so, to isolate the structures and mechanisms that operate to intervene to successful policy

implementation and use. By presenting the categories we uncovered at Beta, our intention is not to suggest that these categories are universal. Indeed, the frames are dependent on space and time. However, in this specific case, the aforementioned categories could explain the experienced adversities around InfoSec policies and, by relating the categories to a wider social theory [15] our findings might be meaningful to other cases beyond the confines of this specific case.

Information security research that draws on frames is in its infancy. Uncovering the categories that functioned as underlying structures for experienced adversities and policy outcomes is an important step. However, more needs to be done in order to fully understand and appreciate the part that the frames can have in information security. We have continued the journey that was started before us, most notably by Hsu (2009) [11], and wish to suggest some routes for further journeys. The formed frames tend to be persistent and hard to change, but effective means for shaping and reshaping the frames are needed. Earlier research in frames has suggested that visible signs and training can have an impact on frames [9]. Despite the research efforts on information security awareness (see [24] for review), no research has addressed effective information security awareness initiatives that could shape employees' frames. Further, we suggest that information security research would benefit from an increased understanding of how frames shift in salience during implementation of information security practices. Lastly, since it is likely that different categories are in effect in different time and space, investigating how the frames (and their categories) are shaped and reshaped during, for example, InfoSec policy implementation process, could open insights into how the frames affect InfoSec policy implementation. We argue that only through more thorough understanding of the workings of frames on information security, better practices can be introduced.

Our research was initiated by practical relevance; information security professionals who had implemented InfoSec policies sought for better understanding for the adversities and unexpected policy outcomes at their organization and wished for better information security management practices. From practitioner perspective, our study's aim was to provide insight for IS managers, struggling with their information security practices, on ways to enhance and improve their practices. Based on our conceptual framework and empirical findings we suggest that to achieve expected policy outcomes the ISPFORs need to approach congruence. To analyze incongruence, the groups' frames need to be made explicit. In this paper, we have brought forward the methodological steps to uncover and make explicit the categories for others to repeat.

As a practical contribution from our analysis, we were able to provide insight for the involved IS managers. For example, to achieve expected policy outcomes, the InfoSec professionals at Beta should be present in the everyday work of those who need to translate the espoused theory into theory-in-use. Although our practical suggestions are highly idiographic, we argue the concept of ISPFOR is not only confined and of practical use to the IS managers at Beta, but to a wider group of IS managers. Most importantly, our analysis of the importance of perceptions and of their effects on overall information security, we contributed to practice by suggesting that listening, not just hearing, what the organization wants to say, pays off also in information security management.

## 7. Conclusions

While InfoSec policies form the foundation for information security in an organization, policy implementation continues to be challenging for IS managers. The InfoSec policies are exposed to a number of stakeholders who have differing interest in and concerns relative to the policies. In this study, we have proposed the concept of ISPFOR to explain how the socio-cognitive structures shape perceptions of InfoSec policies and how these underlying socio-cognitive structures can explain adversities and unanticipated policy outcomes. The concept was applied in an interpretive case study. Our findings suggest that employees' interests and interaction with the policies affect how policies are perceived and the perceptions contribute to the success or failure of the policies. The ISPFORs functioned as the underlying structures and mechanisms that explained the adversities and unanticipated policy outcomes. Therefore, emphasizing the architectural factors of the InfoSec policy documents or employee compliance is not sufficient but needs to be augmented with an understanding of organizational groups' perceptions of InfoSec policies. The findings may be intriguing not only for researchers but also for practitioners interested in understanding how InfoSec policies should be formulated and implemented in order to avoid unexpected outcomes and to achieve expected ones.

## 8. References

[1] R. Baskerville, and M. Siponen, “An information security meta-policy for emergent organizations”, Logistics Information Management, vol. 15, no. 5/6, 2002, pp. 337-346.

[2] B. Bulgurcu, H. Cavusoglu, Hasan, and I. Benbasat, ”Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness”, MIS Quarterly, vol. 34, n. 3, 2010, pp. 523-A7.

[3] E.J. Davidson, “Technology Frames and Framing: A Socio-Cognitive Investigation of Requirements Determination”, MIS Quarterly, vol. 26, no. 4, 2002, pp. 329-358.

[4] E.J. Davidson, “A Technological Frames Perspective on Information Technology and Organizational Change”, Journal of Applied Behavioral Science, vol. 42, no. 1, 2006, pp. 23-39.

[5] G. Dhillon, Principles of Information Systems Security: Text and Cases, John Wiley & Sons, Hoboken, NJ, 2007.

[6] N.F. Doherty, L. Anastasakis, and H. Fulford, “The information security policy unpacked: A critical study of the content of university policies”, International Journal of Information Management, vol. 29, no. 6, 2009, pp. 449-457.

[7] N.F. Doherty, and H. Fulford, ”Aligning the information security policy with the strategic information systems plan”, Computers & Security, vol. 25, no.1 , 2006, pp. 55-63.

[8] J.M. Hagen, E. Albrechtsen, and J. Hovden, “Implementation and effectiveness of organizational information security measures”, Information Management & Computer Security, vol. 16, no. 4, 2008, pp. 377-397.

[9] S.G. Harris, “Organizational Culture and Individual Sensemaking: A Schema-Based Perspective”, Organization Science, vol. 5, no. 3, 1994, pp. 309-321.

[10] T. Herath, and H.R. Rao, ”Protection motivation and deterrence: a framework for security policy compliance in organisations”, European Journal of Information Systems, vol. 18, no, 2, 2009, pp. 106-125.

[11] C.W. Hsu, “Frame misalignment: interpreting the implementation of information systems security certification in an organization”, European Journal of Information Systems, vol. 18, no. 2, 2009, pp. 140-150.

[12] K. Höne, and J.H.P. Eloff, “What Makes an Effective Information Security Policy?”, Network Security, vol. 2002, no. 6, 2002, pp. 14-16.

[13] K. Höne, and J.H.P. Eloff, ”Information security policy - What do international information security standards say?”, Computers & Security, vol. 21, no. 5, 2002, pp. 402-409. (2002)

[14] M. Karyda, E. Kiountouzis, and S. Kokolakis, “Information systems security policies: a contextual perspective”, Computers & Security, vol. 24, no. 3, 2005, pp. 246-260.

[15] H.K. Klein, and M.D. Myers, “A Set of Principles For Conducting and Evaluating Interpretive Field Studies In Information Systems”, MIS Quarterly, vol. 23, no. 1, 1999, pp. 67-93.

[16] S. Kvale, InterViews: An Introduction to Qualitative Research Interviewing, Sage Publications, Thousand Oaks, CA, 1996.

[17] A. Lin, and L. Silva, “The social and political construction of technological frames”, European Journal of Information Systems, vol. 14, 2005, pp. 49-59.

[18] J. Lindström, and A. Hägerfors, ”A model for explaining strategic IT- and information security to senior management”, International Journal of Public Information Systems, vol. 1, 2009, pp. 17-29.

[19] M.B. Miles, and A.M. Huberman, Qualitative Data Analysis: an expanded sourcebook, Sage Publications, Thousand Oaks, CA, 1994.

[20] W.J. Orlikowski, and J.J. Baroudi, “Studying Information Technology in Organizations: Research Approaches and Assumptions”, Information Systems Research, vol. 2, no. 1, 1991, pp. 1-28.

[21] W.J. Orlikowski, and D.C. Gash, “Technological Frames: Making Sense of Information Technology in Organizations”, ACM Transactions on Information Systems (TOIS), vol. 12, no. 2, 1994, pp. 174-207.

[22] P. Oscarson, Actual and Perceived Information Systems Security, Linköping University, Linköping, Sweden, 2007.

[23] Pricewatercoopers, Information Security Breaches Survey 2010: technical report, 2010.

[24] P. Puhakainen, and M. Siponen, ”Improving employees' compliance through information systems security training: an action research study”, MIS Quarterly, vol. 34, no. 4, 2010, pp. 767-A4.

[25] M. Siponen, and J. Iivari, “Six Design Theories for IS Security Policies and Guidelines”, Journal of the Association for Information Systems, vol. 7, no. 7, 2006, pp. 445-472.

[26] M. Siponen, and A. Vance, ”Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations”, MIS Quarterly, vol. 34, no.3 , 2010, pp. 487-A12.

[27] M. Siponen, and R. Willison, ”Information security management standards: Problems and solutions”, Information & Management, vol. 46, no.5, 2009, pp. 267-270.

[28] K. Dunkerley, and G. Tejay, “Theorizing information security success: towards secure e-government”, International Journal of Electronic Government Research, vol. 6, no. 3, 2010, pp. 31-41.

[29] S.H. von Solms, ”Information Security Governance - Compliance management vs operational management”, Computers & Security, vol. 24, no 6, 2005, pp. 443-447.

[30] R. von Solms, and B. von Solms, “From policies to culture”, Computer & Security, vol. 23, 2004, pp. 275-279.

[31] J.P. Walsh, “Managerial and Organizational Cognition: Notes from a Trip Down Memory Lane”, Organization Science, vol. 6, no. 3, 1995, pp. 280-321.

[32] G. Walsham, “Interpretive case studies in IS research: nature and method”, European Journal of Information Systems, vol. 4, no. 2, 1995, pp. 74-81.

[33] M. Warkentin, and A.C. Johnston, ”IT Governance and Organizational Design for Security Management” in D.W. Straub, S. Goodman, and R.L. Baskerville (eds.), Information Security: Policy, Processes and Practices, M.E. Sharpe, Armonk, NY, 2008.

[34] M.E. Whitman, ”Security Policy: From Design to Maintenance”, in D.W. Straub, S. Goodman, and R.L. Baskerville (eds.), Information Security: Policy, Processes and Practices, M.E. Sharpe, Armonk, NY, 2008.