ISM: Irrelevant Soporific Measures

Giving Information Security Management back its groove using sociomateriality

Aahd Kanane
Casandra Grundstrom
Abstract

Information security management is now a major concern for any organization regardless of its type, size, or activity field. Having an information security system that ensures the availability, the confidentiality, and the integrity of information is not an option anymore but a necessity. Information security management identifies difficulties with user behaviour and compliance that is centralized around policies, perceptions, and practices. In order to address how they affect information security management, these three issues are holistically explored using a sociomaterial framework to engage the understanding of human and nonhuman components. A case study of a university in Sweden was conducted and it was found that despite the sophistication of the IT system, human behaviours are a pertinent component of information security management, and not one that can be ignored.

Keywords: information security management, sociomateriality, users’ compliance, information security in public organizations.

1. Introduction

Information is today the most important and critical asset in organizations (Hedström, Kolkowska, Karlsson & Allen, 2011; Torres, Sarrieji, Santos & Serrano, 2006). The strategic value of information is increasingly convoluted and the risks of transgression are increasing as technology advances. This implicates information security to be a strategic issue for all organizations regardless of their size or field of activity since their reputation and reliability is staked upon the effectiveness of their information security (Hedström, et al., 2011; Torres, et al., 2006; Dhillon & Backhouse, 2000). Making Information Security Management (ISM) a top contender in the list of critical elements to be addressed in the management of all kinds of organizations.

Public organizations in particular are usually looked at as less efficient than private organizations in regards to all the facets of their management (Rainey, 2009). But when it comes to ISM, public organizations have a larger and more accurate data reserve about citizens, businesses, and governmental organizations (Bishop, 2003). Also, public organizations are, by definition expected to serve and protect citizens’ rights and interests. Which implies, inter alia, dealing with their information with an extreme level of responsibility and carefulness. Therefore, ISM is required to be as effective in public organizations, if not more, as in any other kind of organization.

Additionally, public organizations are required to meet a considerable level of openness that allows the public to access organizations’ records and official documents. ISM in this particular context needs to be addressed in an ingenious and challenging way (Atkinson, et al., 2012; Fyffe, 2008) which can not in any case fall into the facility of closing or reducing the access to public organizations.

Extant research is mainly focused on the technical level as ISM was perceived for a long period of time as a set of procedures that once implemented will achieve information security (Dhillon & Backhouse, 2000; Zafar & Clark, 2009; Siponen & Oinas-Kukkonen, 2007). More recently, a rise in the socio-organizational perspective applied to ISM is observed (Zafar &
Clark, 2009; Siponen & Oinas-Kukkonen, 2007). This emerging approach allowed the investigation of human and context related issues to ISM that affect the security of information just as much as the technical factors (Dhillon & Backhouse, 2001; Siponen & Oinas-Kukkonen, 2007). Research in this sense has shown that one of the main challenges facing ISM is users’ compliance with ISM policies (Zafar & Clark, 2009, Siponen & Oinas-Kukkonen, 2007; Hedström, et al., 2011). Three sources of this issue were examined by researchers. One source is the policies and how they are made and implemented. Another source is the users’ perceptions of their role and the role that other users play in ISM; also their perceptions related to the policies and their importance. The last source is the users’ practices and priorities while performing their daily activities (Zafar & Clark, 2009; Siponen & Oinas-Kukkonen, 2007; Hedström, et al., 2011).

The implications for both organizational research and practice, when social or technical considerations are black boxed, is a lack of understanding towards how these two constituents embody together organizational events. IS research has been argued to contain both social and material components (Jones, 2014; Orlikowski, 2007) and as such, stands to be an opportunity to engage this issue with the emerging sociomateriality perspective. Adopting this approach takes into consideration both human and technology dimensions and enables the capture of the elastic nature of ISM swinging between human and material agencies (Coles-Kemp, 2009). Accordingly, our research will be focused on the following question:

*How is Information Security Management influenced by policy, perceptions, and practice?*

To answer this question, we have conducted a qualitative case study with a public university to identify policies, perceptions, and practices that affect ISM. Upon identification and understanding of the effects of these 3 considerations through a sociomaterial lens, we can generate knowledge for not only other universities in similar contexts, but other public organizations as well. Our generation of new understanding within the ISM field stands to offer not only the practical application to university security, but theoretical contributions towards philosophical sociomateriality within the ISM field.

### 2. Related Research

In our related research section, we look at ISM and the broad definition it encapsulates. We then come to examine a brief history of information security research within organizations and how it was limited to the technical level until researchers confronted literature and its technical focus and concluded that human related factors were being ignored. Hence the need for a most holistic approach which we based on existing research of policies, perceptions, and practices. The second part of this section is our framework and introduces sociomateriality as a lens, argues for why it is an appropriate approach, and defines important constructs pivotal to our thesis.

#### 2.1 Information Security Management

ISM is usually used to indicate the discipline that covers the protection of information related assets from different risks ranging from theft to damage. It enhances the organization’s ability to adapt to its new environment full of risks that threaten its credibility and security (Caralli & Wilson, 2004; Firesmith, 2003; Torres, et al., 2006; Von Solms & Von Solms, 2005). Despite intensive research in ISM field, it remains problematic to pinpoint a comprehensive and
common definition of what information security is (Zafar & Clark, 2009). Nevertheless, there seems to be an agreement on its objective to preserve the availability, the confidentiality, and the integrity of information (Zafar & Clark, 2009; Siponen & Oinas-Kukkonen, 2007; Bishop, 2003).

For several years, information security research was limited to the technical level of ISM neglecting the conceptual and organizational levels. One reason behind this, is that information security was considered as a purely technical issue and commonly accepted as so. As a result of this understanding research purposes were aligned with the technical considerations of information security. Another reason is that information security research was shaped by the various schools of thought within information system research (Siponen & Oinas-Kukkonen, 2007).

In this regard, Dhillon and Backhouse (2001) confronted the literature related to information systems and information security and analyzed the evolution and the directions of information security research. By using the Burrel & Morgan framework, four paradigms were selected by using the dimensions of regulation and radical change: the functionalist paradigm, the interpretative paradigm, the radical humanist paradigm, and the radical structuralist paradigm.

The Dhillon and Backhouse (2001) study shows that information security research is focusing mainly on the technical part of information systems. For instance: checklists, risk analysis and evaluation, technical standards, access control and so on (Dhillon & Backhouse, 2001; Siponen & Oinas-Kukkonen, 2007). Their study also shows that the majority of the research considers that information security has delimited boundaries regardless of its environment. Another result is that ISM is perceived as a defined process with specific inputs, outputs, and evaluation mechanisms. Once this defined process is correctly implemented information security will be achieved (Dhillon & Backhouse, 2001) giving minimal consideration to the context or users’ compliance.

With that being said, there is an increasing number of researches that are going toward a socio-organizational perspective in information systems that combines technology, culture, and organization. However, when it comes to managing information security, research seems to stagnate in the technical side and fail to address the human related questions such as behaviors, practices, and context (Dhillon & Backhouse, 2001; Zafar & Clark, 2009; Siponen & Oinas-Kukkonen, 2007). The reason behind this focus on the technical side according to Dhillon and Backhouse (2001), is that the majority of the conducted research pertained to the functionalist paradigm which considers that security is concrete and tangible. Even if this functionalist paradigm is becoming a largely debated upon topic and that there is an increasing movement towards the socio-organizational perspective; in addition to the recognition of the importance of addressing the social issues, most of information security research is still limited to the processes and controls.

In the same direction, Zafar and Clark (2009), conducted a study where they reviewed all the papers published in the nine big journals of IS research from the day of their inception to 2007. During this study they found that there is a significant increase in the publications dealing with information security since 2000. Furthermore, by using the information security capability model that addresses the technical, behavioral, and managerial concerns related to information security, the results of their review converges to a great extent with the Dhillon and Backhouse (2001) study. Their conclusions puts forth the need to break away from the technical orientation of current research and aim for a more holistic approach that will allow researchers to consider ISM as a whole. ISM has to be looked at in its entirety by taking into consideration all its aspects and the connections between them.
After that the need for orienting research towards a more holistic approach that takes in consideration all the elements of ISM was established, several scholars started to go beyond the technical level of IS research to explore more the organizational level by investigating the human and context related issues in ISM (Chan, Woon, & Kankanahalli, 2005; Mishra & Dhillon, 2006; Bulgurcu, Cavusoglu & Benbasat, 2010). Extensive literature reviews performed by Mishra and Dhillon (2006) and Bulgurcu, et al. (2010) showed that there is a considerable and growing stream of research focusing on users’ behavior and compliance with safe ISM practices in particular among any other issues.

Looking at the specific issue of users’ behavior and compliance with ISM policies, several studies (Bulgurcu, et al., 2010; Curry, Marshall, & Kawalek, 2014 ; Chan, et al., 2005; Hedström, et al., 2011; Kraemer, Carayon, & Clem, 2009; Mishra & Dhillon, 2006) addressed the origin of this issue. The results rotate around three factors: the policies, the perceptions, and the practices. Users’ compliance with safe ISM policies depend upon on how those policies are developed, communicated, and implemented. It also depends on the users’ perception of: the importance of ISM policies, the consequences of their behavior and the different levels of risk they undertake, the management attitude and measures regarding security, and the responsibilities and prerogatives of other employees in different departments or hierarchical levels regarding information security. Finally, practice depends on the nature of the users’ daily activities, the priorities they have while accomplishing those activities, and how they perform them.

Despite all the aforementioned factors that prevent the conversion of ISM policies and procedures to practice, research has mainly focused on using controls and punishment measures to force users’ compliance (Mishra and Dhillon, 2006). Rather than exploring ways that have better chances of succeeding and that are more aligned with the users’ perceptions and practices.

In short, extensive IS research has examined the technical side of ISM at large while the social aspects were addressed in a limited fashion with hardly any research considering both elements. Research has limited understanding of the issues regarding users’ behaviour and compliance towards ISM, especially at the intersection of social and technical elements. Furthermore, by looking at policies, perceptions, and practices inclusively, not only the relationship between the elements that have been previously separated in research is established but the avenue for addressing information security issues from a holistic perspective is engaged.

2.2 Sociomaterial

The digital era has brought forth the challenge of explaining, evaluating, and examining the relationship that exists between organizational life and information technology (IT) (Leonardi & Barley, 2008; Leonardi, 2013; Mutch, 2013). In a literature review of 4 leading management journals conducted by Orlikowski and Scott (2008: 434) it was determined that “over 95% of the articles published in leading management journals do not consider or take into account the role and influence of technology in organizational life”, leaving only 100 of the 2027 analyzed articles that actually focus on ‘technologies’ impact on organizations. This ‘absence presence’ as characterized by Orlikowski (2009), is quite astoundingly absurd as technology is ubiquitous in everyday life and organizations are no exception.

There are two further established perspectives that can be included under the canopy for how technology appears in management research. The first of the two marks technology to be an independent force in organizational change. Distinctly labelled as an ‘exogenous force,’ it
has a certain and calculable impact on organizations and further considers technology as simply hardware (Orlikowski, 2010; Brynjolfsson & Hitt, 1996). The second perspective contends to consider human influences in terms of actions, choices, or contexts that are influenced by the behaviors of an individual which is termed ‘emergent process’ (Orlikowski, 2010). In dispute with an ‘exogenous force’ it is tilt away from technology to look at the human components of technology in organizations.

In other words, technology in management has either been vastly ignored, or flip-flopped to focus on either the technology or on the human context. In the last 2 perspectives, each could be said to have the weakness that the other holds as a strength, exogenous force ignores the role of the human context, whilst the emergent process neglects the inclusive effects of technology as a dynamic artifact (Orlikowski, 2010; Orlikowski & Iacono, 2001).

As a result of the aforementioned perspectives, sociomateriality has emerged as a controversial approach to study Information System (IS) and is a heavily deliberated upon topic among scholars (Leonardi, 2013; Leonardi, Nardi, & Kallinikos, 2012; Orlikowski, 2010; Orlikowski & Scott, 2008). Sociomateriality, the intentionally blended terms of ‘social’ and ‘materiality’ signals an ontological amalgamation, a means to entwine social agents and material artifacts that are typically treated as separate entities (Orlikowski, 2007; Orlikowski, Golsorkhi, Rouleau, Seidl, & Vaara, 2010; Orlikowski & Scott, 2008; Marabelli & Newell, 2012; Leonardi, Nardi, & Kallinikos, 2012). Perhaps best said by Orlikowski (2007: 1437) “the social and the material are constitutively entangled in everyday life.” Not be confused with technology, as sociomaterial is the practice of which technology is encapsulated within (Leonardi, Nardi, & Kallinikos, 2012).

It is worth emphasizing that the definition of materiality is quite important although tricky to really place a neat box around. As defined by Leonardi et al., (2012: 42) materiality is “the arrangement of an artifact’s physical and/or digital materials into particular forms that endure across differences in place and time and are important to users.” More clearly put, materiality “direct[s] attention to the properties intrinsic to technological artifacts” (Leonardi, Nardi, And Kallinikos, 2012: 32) that allows scholars and researchers to distinctly point out properties of artifacts over time and in context. Barad (2003: 802), perhaps best illustrates the critical importance of materiality by expressing “it is vitally important that we understand how matter matters.”

Since sociomateriality will be used as a lens for this study in order to gain insight into ISM, it is important to clearly define and apply the terms that will be used throughout the remainder of this paper. As sociomateriality is an emerging perspective (Leonardi, 2011; Orlikowski & Scott, 2008) there is not a solidified definition of sociomateriality that clearly states when and how it should be used (Jones, 2014). Instead, sociomateriality has components that will be defined and used in this study as “it is unlikely to be possible to define its contribution in more than quite general terms” (Jones, 2014: 921). When defining the constructs, strong sociomateriality afforded the opportunity to understand how processes are shaped from a firmly entangled view. Weak sociomateriality however, is a better fit since the aim of this paper is to explore the ‘how’ of something; the idea of weak sociomateriality enables understanding of individual constructs as they are threaded through a larger picture. Weak sociomateriality sets to “focus more on how social and material agencies combine” (Jones, 2014: 922) which then implicates the imbrication of their sociomateriality for organizations (Leonardi, 2013). The following table presents the sociomaterial constructs, their definitions, and how they apply to the ISM context.
<table>
<thead>
<tr>
<th>Construct</th>
<th>Definition</th>
<th>Applications to ISM</th>
<th>References</th>
</tr>
</thead>
</table>
| **Sociomateriality** | The execution of particular actions that mingle social phenomena with materiality | The understanding of how ISM activities mingle materiality with social phenomena | Orlikowski, 2007  
                           |                                                                             |                                                    | Orlikowski & Scott, 2008  
                           |                                                                             |                                                    | Leonardi, Nardi, & Kallinikos, 2012  |
| **Social**   | Abstract notions that are created through processes such as: policies, standards, norms etc | Insight into the concepts that shape ISM through social contexts: policies, procedures etc | Leonardi 2012  
                           |                                                                             |                                                    | Leonardi, Nardi, & Kallinikos, 2012  
                           |                                                                             |                                                    | Leonardi 2013  |
| **Materiality** | When a physical or digital artifact holds importance to a user over time and dimension | Perceptions of physical and digital artifacts that mould ISM: data storage/retrieval, centralized systems | Leonardi 2013  
                           |                                                                             |                                                    | Orlikowski & Scott, 2008  |
| **Imbrication** | A metaphor to describe the relationship between the social and the material to show interdependent functionality and response | Ability to understand the social and material components of ISM to be interwoven together and therefore to be extractable for introspection and comparison | Leonardi, 2011; Leonardi & Rodriguez-Lluesma, 2012; Leonardi, Nardi & Kallinikos, 2012  |
| **Constitutive Entanglement** | A relational ontology of the social and material | Minimizes one and two way actions of the social and material within ISM so that they are inextricably linked | Orlikowski 2007 |
| **Artifact** | Physical or digital ‘things’ that are shaped by human and/or social interactions | Awareness of tangible and digital components that comprise ISM | Robey, Raymond, & Anderson, 2012  |
| **Human Agency** | When one establishes and comprehends a goal(s) | How humans engage with technology’s material agency to form/achieve a goal | Emirbayer & Mische 1998; Giddens 1984  |
| **Material Agency** | The existence of nonhuman entities | The understanding of how technology's | Pickering 2001; Volkoff, Strong, &  |
that can act separate from human interference | materiality acts within ISM | Elmes, 2007 |
Social Agency | Human operations that are intentionally formed to realize goal(s) | The social nature of how material agency is enacted through goal seeking in groups | Pickering 2001 |
Practice | The area through which social and material are treated through the imbrication process to become constitutively entangled | Enable empirically observable entities of technology and organizations | Leonardi 2012 |

Table 1: Sociomaterial Framework

It is important to note, that although our research question focuses on three sources of ISM issues. Sociomateriality is a way for us to centralize our research for a holistic understanding by considering both human and nonhuman factors.

3. Methods

In this section, the research design is presented. In the first part the choice of using a case study is motivated and then the case is presented. After that, the data collection and analysis processes are described. Finally, some limitations related to the method used are presented.

3.1 Case Study Method

An indispensable and widely accepted method to contribute to IS research is case studies (Klein & Myers, 1999; Alavi & Carlson, 1992). The case study approach allows researchers to appropriate a holistic view within organizational and social contexts (Yin, 2009; Klein & Myers, 1999) as well as addressing explanatory questions (Yin, 2009). Furthermore, case studies carry with them empirical inquiry that look at specific phenomena in social contexts that might be indistinguishable from one another otherwise (Yin, 2009). For these reasons, a case study method is appropriate for our research in 3 distinct ways:

1) To understand how ISM is influenced, looking towards a comprehensive view of the organization will help us to generate an interpretive picture,
2) by looking at specific phenomena, policy, perceptions, and practice, their empirical qualities further engage with the sociomaterial framework, and finally
3) the explanatory power of a case study, complements the research question.

This approach is not without its caveats however, and in the interest of showing the quality of our case method, we will briefly address Yin’s (2009) suggested tests of case study methods. These are: construct validity, internal validity, external validity, and reliability. The following section is based on definitions by Yin (2009):
1) Construct validity: the concept that is to be studied must be grounded in (optimally) several sources of evidence.
2) Internal validity: proof on internal concept following predicted outcomes.
3) External validity: the case study generalization is limited by context.
4) Reliability: the study should be replicable in terms of similar results.

With these 4 caveats in mind, the following is a respective list of how we plan to address these 4 issues:

1) Construct validity: our related research and framework is all grounded in multiple sources that comes from peer reviewed journals, nor are unfounded claims made.
2) Internal validity: as we were not testing a hypothesis, nor did we influence the internal working of the case, this is not a relative concept for our case study.
3) External validity: generalization has long been a concern for case studies (Yin, 2009), and as our results may prove not to be generalizable within other areas, because we are studying a university that has similar context all throughout the geographic location of Sweden. We will address that generalization is restricting but not irrelevant for other universities outside of the case directly studied.
4) Reliability: Throughout our entire process, and particularly in the method section, we have been transparent with how we approach all considerations. Although there are some problems with language, it is possible that a Swedish interviewer could reveal more in depth discussions with the respondents in their native language. Despite this, we feel that the core concepts have been grasped and documented with as minimal amount of bias as possible.

To summarize, although case studies do have concerns, we have addressed these problems head on, and discussed them explicitly. The case study method complements our research, in more ways than one, and is particularly well suited to IS research (Klein & Myers, 1999; Alavi & Carlson, 1992). Furthermore, as we will be using a sociomaterial framework, the abstract notions of sociomateriality are difficult to apply without grounding them in a setting, for us, this setting is the case study (Jones, 2014).

3.2 Case Description

In order to approach the influence of policies, practices, and perceptions on ISM within public organizations, the case of a university in Sweden was studied. This university has 4,335 employees and 31,506 students which means that approximately 35,840 users interact with the information system.

As a public organization, the university has to comply with governmental requirement regarding the management of personal data. Also, its ISM system has to meet the expectations of different kinds of users with different needs, levels of adaptation capabilities, awareness, and ease using technology. All this in a context where information is supposed to be public and freely accessible by everyone.

3.3 Data Collection and Ethical Considerations

In order to help define the focus of our research, an exploratory interview was conducted first with a respondent from the intermediate level of the responsibility line. This interview enabled us to understand the state of ISM in the university, gain insight on ISM challenges faced by both top management and users, and identify potential paths to consider for the research.

Based on the findings of the exploratory interview a semi-structured interview guide was organized around five themes: role and personal background, daily routines, understanding of
information security, understanding of sensitive information, and information security awareness. This interview guide was then used for 4 semi-structured interviews with 7 respondents from different sides of the organization both technical and business related, and different levels of responsibility line.

The process of selecting respondents was carried out based on a referral process among respondents and conducted by calls and emails to different employees working in different areas of the organization. This process allowed us to contact 20 individuals and we conducted interviews with all those who accepted to take part in the study. Except for the respondents from the external vendor who were present during respondent 2’s interview and circumstantially accepted to participate in the interview.

We use the term ‘user’ to refer to individuals who interfere with the university’s information system and that are in the low level of the responsibility line such as respondent 3. The users may or may not be aware of their impact on ISM. The following tables illustrates the distribution of the respondents in terms of responsibility and focus:

<table>
<thead>
<tr>
<th>Responsibility line</th>
<th>Technical focus</th>
<th>Business focus</th>
<th>External stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Respondent 2 (R2)</td>
<td>Respondent 4 (R4)</td>
<td></td>
</tr>
<tr>
<td><strong>Intermediate</strong></td>
<td>Respondent 5 (R5)</td>
<td></td>
<td>2 respondents from an external vendor (EV)</td>
</tr>
<tr>
<td></td>
<td>Respondent 1 (R1) (exploratory)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Respondent 3 (R3)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: An overview of the respondents distribution

The choice of using semi-structured interviews was made because they are “best suited for the exploration of the perceptions and opinions of respondents regarding complex and sometimes sensitive issues,” (Barriball & While, 1994). Using themes enabled us to focus on standard questions and limit the disparities in the answers between respondents to their opinion and not to their understanding of the purpose of question. Semi-structured interviews allow as well to compare the answers of the respondents during the analysis (Cohen and Crabtree, 2006).

All the interviews were performed in person, this approach enables the exploration of the attitude, values, and motives of the respondents. It also helps ensuring that the respondents answer all the questions without being influenced by external factors such as peers. Also, all the interviews were recorded with the respondents’ consent to ensure the precision and integrity of the data collected and to reduce the risk of errors and misinterpretations (Barriball & While, 1994).

It is worth noting that during the data collection process we gave a particular attention presenting to every respondent the topic and the goal of the research, making sure that they understand what the data collected will be used for, and that no personal information such as names, gender, or age was saved.

The main challenge when conducting those interviews was that English is the second language for all the respondents. Difficulties related to the language were palpable in some
interviews more than others without affecting the validity of the results since the nature of semi-structured interviews allow rephrasing the questions and making sure that the respondents understand the question before answering it.

All the interviews were transcribed verbatim and some corrections for grammatical considerations were applied to parts of the transcripts before analysis. Those corrections are indicated in the quotations with the standard square parentheses.

3.4 Data Analysis

The data collected from the interviews were subject to three layers of analysis. First, all the transcriptions were coded, the codes helped organizing the data by building storyboards for each interview and excluding irrelevant parts of the transcriptions before applying the sociomateriality lens.

Then, an initial analysis of the codes using all of the sociomaterial constructs (10) allowed us to narrow down and identify five sociomaterial constructs that shaped the analysed data. The purpose of the codification is to provide a set of rich statements that can have the sociomaterial framework applied to them (Jones, 2014).

This step is not to say that the other constructs were not important or did not reflect within the data, but their presence was not justifiably influential when considering our research question. The retained constructs were: sociomaterial, material, social, social agency, and imbrication.

Once the critical constructs were identified, we then used those constructs on the analysed data to identify issues related to each construct. To bring the data to an aggregated level, the last step involved using the identified issues as they were grouped in their constructs. The following table illustrates an overview of the final step of the analysis in terms of identified issues and the sociomaterial construct used in the approach.

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Quote</th>
<th>Issues described</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sociomaterial</td>
<td>“We don’t have many systems where we log like personal and data or something and if we had those then maybe the question would pop more often, maybe I would hope so at least. But still, I don’t think we talk about it much even in terms of other data because it could be sensitive.” R3</td>
<td>The nature of the information system does not necessitate considering ISM</td>
</tr>
<tr>
<td>Materiality</td>
<td>“They need to classify the data here. To protect it is not the problem I think. The classification is the problem.” EV</td>
<td>Data classification</td>
</tr>
<tr>
<td>Social</td>
<td>“If you have people that doesn’t bother giving some other their login, they will do it at the university too...” R4</td>
<td>Users behaviour</td>
</tr>
<tr>
<td>Social agency</td>
<td>“In the [unnamed] department, we have designed our own systems to help us [...] and different departments do their own stuff.” R1</td>
<td>Lack of standardization</td>
</tr>
</tbody>
</table>
Table 3: An overview of the analysis final step

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Imbrication</strong></td>
<td>“There [are] a lot of expectations in the organization that information is, is, public always! I should have access to it, why don’t I?” R5</td>
</tr>
<tr>
<td><strong>Managing access expectations</strong></td>
<td></td>
</tr>
</tbody>
</table>

### 3.5 Limitations

Centralized to this thesis is the case study which is based upon a single university and upon one source of information which are interviews. Also, the study is based upon a small empirical sample within a large organization considering only one respondent for the users’ perspective and a greater focus upon management. This ultimately means that the results of this thesis cannot be generalized. However, we see that despite of this, case studies are a valuable method for generating understanding through the studies that they are composed of, although, they cannot make predictions (Walsham, 1995). Furthermore, in the case of a Swedish university, there are many other universities that may see this study as a valuable explanation as they too are within the public organization context.

### 4. Results

In this section, the outcomes of the analysis process using five sociomaterial constructs are presented.

#### 4.1 Sociomateriality

Using a sociomateriality lens we noticed that there is a disparity in understanding towards what ISM means for the organization. We discerned that the respondents in the management level are aware that IT solutions are not enough to address ISM issues properly but still, there is focus on the technical side since they failed to integrate other levels of users when changing their behaviors and contributing to improve ISM understanding within the organization.

“[...] we need an organization that understand what information security is not just a policy or group talking about information security we need a real information security person we mandate to affect the rest of the organization and when we have that in place it will be easier for the technology to support that, but unless we have that well then the technology need to do what it can to support information security.” R5

“It is about behavior and I would normally say that” R4

“The most important thing for the departments is to have backups of data” R2

“If you want to have security you need to have control.” R4

“It’s not about stopping people, it is about helping people... People are people, they do these mistakes [...] but I want to make sure that the consequences are not so bad.” R2

Looking towards how ISM is then addressed within the organization is shown in two lights. The first, that management’s formal use of ISM lies within policies.

“[...] it is used on the top levels on the strategic level, our policy documents.” R2
“It’s a problem to make sure that all staff reads the policy documents... they are boring... but that is real life.” R2

However, on a more practical level, the use of ISM is far less formal.

“[...] I don’t think we talk about it much even in terms of other data because it could be sensitive” R3

The fundamental reason why management is contending for ISM, even just at the technical level, is because the domino effect that losing control over information in the university will bring about consequences.

“[...] because it’s about the integrity this institution and it’s so so so important, because if people don’t believe in us, if they don’t trust us, then we will not get any money for research and students don’t want to be here because it’s a mess.” R2

Losing institutional credibility gives a central reason for management and users to engage in ISM. However, respondents identified different issues within ISM and the response was either a technical or social concern depending on their role and level in the hierarchy. For instance respondents with technical roles higher in the hierarchy tend to emphasise storage and accessibility issues, securing data in the cloud, personal devices security while other users restrict their answers to classification, routines and behaviors. However, all respondents identified hacking, phishing mails and level awareness and education as part of the most critical issues facing ISM.

Considering how policies are made, understanding where the decisions come from is essential. For some of our respondents, the decision making line is a top-down approach.

“We have rules and policies decided [by] our director, that this is the way that we are working.” R4
“I am going to say top-down decision, because they [users] are not aware of it.” R4

But the communication effectiveness of these policies falls short in reaching users.

“[in regards to updated policies] Yesterday, I talked to a person fairly up in the organization who haven’t even seen the message.” R5
“No, I haven’t seen any policies, maybe there are but I’ve never seen them. No one told me.” R3

The other decision making line comes from a more technical respondent, where decisions are made based on user feedback.

“Feedback, all the time!” R2
“We have a continual discussion with the staff [...]” R2
Yet when users feedback is solicited, users believe that their opinion is not important.

“there was some sort of document [...] asking a couple of questions about information security. I think my boss and I looked at it and we tried to answer it [...] apparently we got an answer back that they said that it was not that important. So don’t bother.” R3

Sociomateriality showed that there are policies that formally address ISM, which while aimed to help govern, also are used for understanding. However, the respondents within management understand that these policies and procedures are largely ignored and that there is a need for changing users behavior and for adopting appropriate routines.

“It is like traffic [...] it doesn't help when you teach people how to drive, they still drink and drive.” R2

“[...] normally it’s compared to the traffic. You have a driving license, and you have it because you are supposed to do it in a special way and behave. Even though you don’t behave, all people don’t behave. You drive too fast, and you do whatever you want. And we are building the streets, because with people, with us they misbehave. And it’s the same people that we have here. Some of them won’t, they will never [...] and we have to see that it’s, I mean if it’s just part of himself or herself, then okay, they have a problem. But for us, the most important to see the whole department will have problems within it.” R4

“We should have routines for many things and about security it isn’t just a possible threat nowadays, it is a threat and I guess it’s easy to always that ‘oh well it doesn’t happen to me’ or that the data I am using is not that sensitive or something like that.” R3

Behavior of users is also reflected on a more technical oriented side. In terms of employees complying with such considerations as backup and storage, a manager who is responsible for such an area indicates how by following this policy, users would experience less problems.

“When we talk about backup for example, we have a service for that in our IT because we can say what our responsibility is and we put out a lot of services for the university [...] we can say to each department that if you choose to use the services you don’t have to think about it [...] but they want to do what they want...” R4

The behaviour of being more security conscious is reflected throughout our respondents, chiefly because it is part of their everyday activities.

“I have always struggled for a higher information security and better quality and more safe than sorry! so I don’t like shortcuts.” R5

“Sending and stuff well, I try to remember what I and keep in mind at least when I email stuff and what I attach and what I don’t attach.” R3

Lastly, sociomateriality wove an understanding of the different ideas of what sensitive information is. Formally, sensitive information is officially defined at the management level, and influenced by the government for the university.
“It is officially defined, and sensitive information is something that can correlate to some individual. So information about you as a student, we are very careful about you, information about staffers we are very sensitive about this.” R2
“We use the standard definition from I think Personuppgiftslagen.” R5

Users from different levels are not aware of the existence of the official definition and define information as sensitive according to their background, common knowledge, or what seems important to them. For some, sensitive information is more oriented towards records and research, for others it includes internal mails and course materials.

4.2 Social
For its part, the social lens indicated an increasing attention given by the management to ISM even if it is still more focused on the technical aspect.

“We actually from this year we got a higher budget for information and IT security, more IT security than information security but anyway [...] and that's a good start.” R5

Besides the financial challenge, users acceptance of more strict routines is the dominating challenge in developing ISM.

“[...] it doesn’t matter if people don’t use it [...]” R5
“I mean we work with that, that’s why we are not so famous they don't like us so much. Because this last year this is what we have done we have put things and this gets more problems they are normally used to this will be like this fast and now we put up stops and they get upset so that we do that.” R4
“The university as an organization has been very open with technology and that’s the university, is totally open you can do anything you like [...] that’s been in that way since the internet started and even earlier also but now we are trying to stop some access and that’s something that is not easy to just do and we also are looking for making things less accessible and that is a problem.” R1

Using the social lens we have also found disparities between respondents on whom they believe is responsible for the protection of information. In general, the management level affirms that they can’t take responsibility for everything, and everyone should be responsible for the information they handle, whereas the lower levels put all the responsibility on the management.

“[...] we have often talked about information technology security and I have tried to have our management to understand that is really important with the information and to understand that that is not our issue, it is not our responsibility because we can't take responsibility for this [...]” R4
“it is responsibility often put on the researcher or the teacher, the staff and they manage it best way they can.” R2
“But it all come down to individual responsibility and what kind of knowledge that you have regarding information and who can access it, and who can share it and where it should be placed. So it’s complex.” R5

“Yes, CIO so we have [name] and I guess he is supposed to be responsible for that [...]” R3

Failing to have responsible users, some emphasize the need to put more responsibility on technology.

“we should have technical systems that as far as it can protect users from using the systems in a wrong way or with information that should not be there, but also of course it comes down to written documents, information sharing, introductions.” R5

The challenge for management is to change user’s’ behavior and and make a greater effort in documenting and formalizing procedure, but this is not enough given how the environment of freedom that the university offers is used to justify irresponsible attitudes.

“With the university when it comes to professors and prefects and staff[...] the ‘academic freedom’ expression so widely used expression for everything.” EV1

“If you have people that doesn’t bother giving some other their login, they will do it at the university too [...]” R4

In addition to the freedom context, when the users behave in an inappropriate way regarding information security there are no disciplinary actions that can be or are taken.

“We don’t use force here, we try to persuade people to use the best tools that we support and if you don’t, it’s your responsibility, don’t ask me for help, go somewhere else.” R2

“[...] we don’t have any measures of punishing people.” EV

“There is no real consequences in anything you do [...]” R5

These two previous issues reinforce the fact that as force is ruled out, the only option left for the management to do is change users’ behavior through sensitization.

“How do you change the behaviour in that it’s difficult, so I think that will be the biggest issue for us and writing the documents.” R4

“The problem is what you cannot do and what you are allowed [...] because if you go too hard on security measures people will try to go around them so you need to be very careful.” R2

And all the management can really do is to be prepared for when the users’ behavior toward information security evolves.

“You can read about it [policies] there, instead of saying read this by force so we are prepared to meet them.” R4
4.3 Material
Compared to other kinds of organizations, materiality revealed that the university has a lot left to do in terms of procedures’ development.

“They usually have standards for everything [...] not only written documents about processes and routines [...] they have standard ways of doing everything and there are consequences [...] We don’t have written documents.” R5

Along with this lack of documentation, there are purely technical difficulties like some of the servers and backup systems used.

“It's a mess, just like everything else. We have a file server that we use [...] we said like 5 years ago that we should switch off this file server, and no one did. And we, apparently we still use it. And I'm not really sure if it's backed up properly. But it is, it is sensitive data at least for our organization because its, we store documents there that we need in our everyday works.” R3

Technical difficulties have also evolved in terms of applications for sharing and storing documentation.

“Here at the university we use Microsoft Sharepoint.” R2

Despite having this application for documentation sharing, the routines and documentation processes that centralized around Sharepoint are not utilized by users.

“We have Sharepoint solution [...] but bad routines for using it which maybe that’s why some people stick to the old file server [...] Sharepoint doesn’t work that well because people don’t put their documents there.” R3

Also, the material lens allowed us to comprehend the maturity of the information classification within the organization.

“They need to classify the data here. To protect it is not the problem I think. The classification is the problem.” EV1

“[...] in the university we are not that mature. We don't have classifications, we don’t have them. We don’t have the written papers who should, who is responsible for this and that. We don't have that. We have an information policy, they are updating the information policy. But is the policy used? Is it understood [...] it’s a shame, classification would help my work a lot.” R5
4.4 Social Agency

From a social agency aspect there came to light a lack of formal and written procedures which impedes the users on understanding how to handle ISM.

“If we had better guidelines we could enforce technical systems that made people not as much think about information security but they are forced to information security, but when we don’t have that support then speaking of it describing it in text and trying to educate other becomes more the only way of work[...] recently people have eye openness for information security and IT security.” R5

“I think it’s a gut feeling most of the time, I guess I am aware and others are aware of the Swedish Law of Personal Information... so if I’m supposed to store names and such then most of the people here know that they have to think about it. But that hardly ever happened so it's not a big issue.” R3

Moreover, users developed ‘non official ways’ for executing their tasks when the procedure is less practical or does not exist.

“I can tell you how it works in both the official way and maybe in the non-official way, but if you start work here first it’s two different aspects.” R1

“I think sometimes it follows the formal and I think it does in terms of like [Booking System][...] we are trying to make it more formal and everybody should know who to contact and reach out to. But in other parts, even in that other system. We have summons for formal instructions for the all other systems then it is just mayhem.” R3

Which feeds the slowness of the standardization process and blurs the responsibility lines.

“in the [unnamed] department, we have designed our own systems to help us [...] and different departments do their own stuff [...] ” R1

“We have a problem in this organization, and we haven’t really solved, because we have no one that is in a formal [position] that is formally responsible of any systems.” R3

“We don’t have the written papers who should, who is responsible for this and that.” R5

5.5 Imbrications

Imbrication allowed us to observe that even if having some kind of uniformity between departments in terms of ISM systems, policies, and knowledge, is perceived as a positive and necessary action. However, there are disparities and obstacles in terms of maturity, decision level making, and financial issues that slow this process.

“[...] about standardization [...] we have been struggling with this for years and say why can’t it just be designed this way, it will make it easier.” R1

“[...] it’s natural that if you have department that is specialized in IT that they know more about it [...] ” R5

“We have a security policy that is much better than on the university level.” R1
“If they give us the money, then we do this tomorrow, but we don’t get the money to do this [back ups system].” R4
“It costs a lot of money to make it and it’s a complicated process.” R1

By using imbrication we were also able to include the role played by the specific culture of openness and accessibility of the university. Indeed, there are no rules about accessing information; information is free and is expected to be accessible at all times but this does not exclude that it still needs to be secured.

“This is the university, everything is free.” R2
“it is more about having it accessible all the time, anywhere,[...]. when you work at the university, it is not 8 to 5, that is not our culture, we work all the time.” R2
“ [...] the university mostly information everyone can have it. You are not supposed to say no.” R4
“the idea that’s possible to ask for something that doesn't mean the idea to take it[...] we think that this is very important but it should not be like this because it’s possible to get if you ask for it” R1

Using the imbrication lens to look at the issue of education and awareness especially among students there is a level of inappropriate behavior when considering the openness context of universities.

“Mostly students sending e-mails to the student health care with all kinds of medical information which is not appropriate in a public system as the e-mail it could be [...] anyone can have access to the e-mail system its information is public.” R5
“Well, we have students from different kind of institutions, describing very detailed about abuse. They have seen or someone have abusing them or harassment, it could be drinking problems and whatever, such as an assignment they should do. They probably study psychology or something like that. But that information is in [learning management system], that information should not be in [learning management system], because a lot of people can access that information. Then we need to address it. How can we protect the information?” R5

Another observation made is that users are more interested in understanding ISM only when they are directly affected by ISM problems.

“On the user level it’s more when we have incidents on like phishing, that’s when people understand they have done something bad [...] or they get affected because someone else did something bad but that’s more or less the general little persons view of information security.” R5
“It helps that things happen [...] information can be lost, we have had experience of hacking incidents we have data center crashes... and that of course helps when we want to talk about information security and the issues that we needed to cover.” R5
Whence the rise in interest around ISM.

“[…] that people are working with scientist and they are starting to call and ask how they would back up information for a more security way and 5 years ago they wouldn’t ask me at all. They would just think that it was a really pain in the ass talking about it. It is much more a hot topic for us than it has been.” R4

Despite the rise of users’ interest around ISM the imbrication lens allowed us to examine the lack of incidents reports on the procedural and emotional levels.

“A problem here is that, people don’t want to say that they actually did because it is shameful. And this a problem for me because if they don’t tell the truth, then I have to start a very severe investigation because then the whole department might be hacked. You see it, when I tell them that, they confess with deeds that, but some of these phishing mail are so smart it’s very easy to fall in the trap” R2

“if we are lucky, they go to their boss, […], that announces that there is a problem here, and hopefully it will kick back to the process developers or to me and we can do something about it from here. If we are unlucky they might go do something on their own, because they know best or whatever.” R3

“[…] sometimes I think I am not safe on my own I think that someday we will do that of course we will also be tracked we can send such a good phishing mail but it would be really really embarrassing if I…” R4

5. Discussion

After using sociomaterial constructs to identify all sorts of issues related to ISM the identified issues range from problems related to policy making, to users’ perceptions and practices. Those results were confronted with existing research to build a stronger understanding of how ISM is affected by policies, perceptions, and practice. A reflection is made on the results’ implications for practice and how they extend existing research on the complexity of the contribution of both human and technical factors in the effectiveness of ISM. Finally reflections on potential directions that can be explored are presented.

5.1 Policy

The data analysis revealed that despite the existence of official definitions on what ISM implies or what sensitive information is. Users do not seem to be aware of that either because of their lack of interest in reading policies or because they are not aware of the existence of those policies. That said, there is a considerable lack in the formalization and development of the procedures. Having detailed written procedures and making sure they reach the respective categories of users is a recommended starting point to support the users in their behavior change process (Furnell, 2006).

Having a level of harmony between departments on the technical and social levels allow a greater interaction between the different levels of the organization (Albrechtsen & Hovden, 2009) which largely contributes to the effectiveness and the continuous improvement of ISM. However, despite that both users and management are aware of the benefits of the standardization; it is slowed by financial considerations.
Also, the results show that there is a discord on how policies include users’ feedback even within the management level. While users do not believe they contribute in any way in the policy making process and that their feedback is not taken in consideration. In this regard, it has been argued that inviting users to take part in building ISM policies is the most efficient way to raise awareness within the organization and to prevent managers from building their approach on the wrong basis while making policies (Albrechtsen & Hovden, 2009). This leads to implementing policies and procedures that are aligned with the reality of culture, practices, and level of awareness in the organization.

### 5.2 Perception

The results reveal that the management is increasingly aware of the importance of ISM because of its impact on the organization’s reputation and has therefore allocated a higher budget for information security. Unlike most organizations that prefer losing data than having it accessed by unauthorized people (Bishop, 2003), the main worry for the studied university is data loss. That said, the university focuses more on IT solutions to address ISM issues as it is hard to change users’ behaviors, besides this, policies are not enough to improve users’ behaviors (Hedström et al., 2010; Bulgurcu et al., 2010; Mishra & Dhillon, 2006). Those policies need to be successfully implemented and this “is only possible when individuals are able to align their value system with management,” (Mishra & Dhillon, 2006: 21).

Especially that the university is an open and a free space where every measure has to go through sensitization and if strict procedures are imposed users will always find a way to counter them anyway (Hedström et al., 2010; Torres et al., 2006). This is illustrated by some users’ reluctance regarding the adoption of cloud and document sharing solutions recommended by the university, and their attachment to obsolete systems even if they are not properly backed up and are less safe.

Both the lack of procedures and the users’ lack of interest in procedures create a considerable confusion about the routines to adopt and the reflexes to have when a problem occurs, this blurs the responsibilities around protecting information. This confusion derives from the poor understanding of the different levels’ perspectives on ISM compounded by: the lack of interaction between the users and the information systems’ managers, the difference in the knowledge and the know-how between all users, and the divergence in attributing responsibility (Albrechtsen & Hovden, 2009). The university studied still has considerable work to do in this direction.

Also, the management choice of focusing on the technical side of ISM affects the users’ perception of what ISM is about. They then start to consider that technology is supposed to protect them in all circumstances. Indeed, technology has a considerable contribution in ISM in terms of damage limitation and early detection of problems (Walton, 2006). But when the management gives a higher attention to technology it skews the perception of users on the role that technology plays in the ISM (Curry, Marshall & Kawalek, 2014; Furnell, 2006). It is important to justify the expected effort from the users in terms of ISM regardless of the IT system’s sophistication.

The last observation is the low level of awareness among both students and employees. By making sure that the users are properly informed of the policies and best practices around ISM, the management prepares the users to better support the organization’s security strategy (Furnell, 2006). However, the most striking observation is the lack of incident reports motivated either by shame or unawareness of the consequences of the incident which reinforces the need of working on a security culture in all the levels of the organization.
5.3 Practice

Finally, the data analysis shows two main areas of concern for ISM related issues for the university practices. The first is: the technology for the physical storing of sensitive information at the departmental level and the second is a separation of formal and informal practices when performing tasks related to ISM. Using technology to face the challenges that ISM presents is a common practice (Dhillon & Backhouse, 2001) and is delineated as such in the specific case of departmental storage of sensitive information. Despite the awareness of relying upon a file server that has questionable capabilities of protecting the departments’ information, it continues to be used. Although the reasons for doing this are unclear, and could be related to any number of reasons such as financial, organizational or others. The fact remains that the priorities of the protagonists who influence practical decisions have not prioritized the protection of sensitive information.

The second recognized issue within practice is how information security is performed in users’ daily activities. As indicated by multiple participants, there is both a formal and informal way that information security is dealt with in the university. The formal method for dealing with ISM is grounded in the policies that are used to address ISM from the management (Mishra & Dhillon, 2006; Ward & Smith, 2002); but, users’ are largely unaware of such documents and instead, informally adhere to ideas of ISM from ideas of common sense and practices previously performed. According to Mishra and Dhillon (2006) and Ward and Smith (2002) communication of policies is just as important as is the usefulness of said policies. Even though the university has recently implemented a centralized system where policies can be accessed, there is a lack of communication around its existence.

Furthermore, different departments practice different levels of security even from that of the university. The departments that are more evolved are typically more technically inclined. Management understands that these disparities between departments exist, but there is no one in a formal position, either for information security in the university, nor someone who is formally responsible for systems or documents.

Both of the identified issues for practice are not necessarily a negative issue, but rather offer room for improvement. Considering both issues are unfavorable due to a lack of responsibility, the studied university stands to help formalization of responsibility on multiple levels; by commissioning an information security officer, one who understands that information security is more than just a policy, or a file server. Ownership of systems is an important part of management by encouraging accountability through ownership (Mishra & Dhillon, 2001) and by creating systems of responsibility, information security moves towards involving social and organizational contexts as well (Chang & Lin, 2007).

5.4 Implications for Practice

ISM was considered for a long time as a technical issue and the responsibility of ISM has been misplaced in the IT department. Today, it has been established that ISM is not limited to technology and is not even limited to a department or a category of users. ISM requires certainly a top-down leadership (Walton, 2006) but this does not discharge the users from their responsibilities.

The management responsibility is to document policies in a clear and accessible way and to make sure that all users are aware of good practices and understand why it is important to adopt those practices (Walton, 2006; Bulgurcu, et al., 2010). However, this does not imply that users will just accept and change their behaviors. Indeed, the management has to take into
consideration that users’ compliance is determined by both organizational factors such as policies and the management attitude, and personal factors such as the users’ priorities and values (Chan et al., 2005). Additionally, even if technology based solutions have a huge contribution in ISM but they are highly insufficient to build an adequate ISM system.

5.5 Implications for Research
Our research along with practical implications also has implications for research regarding how information security management can be understood and undertaken for other researchers. Contemporary research has evolved from focussing on technology (Dhillon & Backhouse, 2000; Zafar & Clark, 2009; Siponen & Oinas-Kukkonen, 2007) into a socio-organizational perspective (Dhillon & Backhouse, 2001; Zafar & Clark, 2009; Hedström et al., 2011). Our research not only contributes to the shallow pool of research at the intersection of the two (Coles-Kemp, 2009; Kraemer et al., 2009; Kim & Lee, 2006), but also supports moving beyond a singular focus (human vs. technology) within ISM into a more holistic view. While we do not think that focusing on either technology or socio-organizational concepts as insignificant, but rather that research stands to gain a broader understanding by having researchers address issues in more depth at this intersection for ISM.

The sociomaterial framework used, further pushes the boundaries of current research of sociomateriality in not only the specific area of the ISM field (Coles-Kemp, 2009), and the general IS field (Orlikowski, 2007; Leonardi, 2012; Leonardi, Nardi, & Kallinikos, 2012; Orlikowski & Scott, 2008; Jones, 2014), but also affords to transcend the traditional ideas of research in other arenas. The sociomaterial perspective, while still in its chrysalis stage of emergence (Leonardi, 2011; Orlikowski & Scott, 2008) holds many opportunities in exploration for more than the 5 constructs applied in our research.

And finally, when interweaving three components of users’ compliance issues, policy, perception, and practice, our results entwine and embody larger ideas than just the individual ideas singularly. Throughout our research, we can see that there is a helical relationship between the policy, perception, and practice, and therein this relationship lays the answer to ‘how’ ISM is influenced by them. Compliance (Zafar & Clark, 2009), culture (Chang & Lin, 2007), policies (Bulgurcu et al., 2010), values (Hedstöm et al., 2011; Mishra & Dhillon, 2006), technology (Dhillon & Backhouse, 2000), awareness and responsibilities (Mishra & Dhillon, 2001) all are answers to the question of how ISM is influenced. Even though research already shows recognition in these separate areas as general knowledge, knowing the why opens up the floor for more questions such as what can be done to address them. In order to face the complex issue of ISM it is more about policies, more about perceptions and more about practices; just like it is more about throwing technology at a problem and expecting compliance from users (Dhillon & Backhouse, 2000), and these areas are open to exploring in greater depth to broaden the understanding.

5.6 Limitations and Future Research
The limitations for this research holds to generalizability. Since only one case study was conducted, the results here cannot be generalized (Yin, 2009) to be applicable to other universities. Instead, it acts as a stepping stone to afford the opportunity for other Swedish universities to reflect on the questions raised and how it then applies to their circumstance.

Opportunities for further research in ISM are actionable through many different methods, even within the sociomaterial spectrum there are many avenues left unexplored: affordances, performativity and assemblages to name a few (Leonardi, 2011; 2012). Similar case studies of
universities with the openness context throughout Sweden could only expand on the understanding presented here. Aggregating this idea further, is the concept of approaching ISM in any context with an open mind to how technology and people are woven together and what implications that then brings for ISM.

6. Conclusion

ISM is at the basis of the integrity of any organization, especially when this organization manages considerable quantities of personal data and has thousands of users interfering with its information system on a daily basis. By using sociomateriality as a holistic approach to ISM issues faced by a university in Sweden, this paper discusses the necessity to go beyond technology based solutions for ISM problems. An approach proven ineffective both by literature and in practice.

This paper presents issues related to three main factors in ISM. First, issues related to policies, how they are made, communicated, and implemented. Then, issues related to users’ perceptions around the importance of ISM policies, the consequences of particular behaviors, the management attitude and measures and information security responsibilities of other employees or departments. Finally, issues related to practice such as users’ daily activities, how those activities are performed, and the users’ priorities while performing their tasks.

The study revealed that even when considerable efforts are made in terms of installing advanced technological solution, the ISM structure remained very weak. The most prevalent issue is users’ awareness and compliance with the recommended ISM practices. Therefore, it is important to give a particular attention to users and include them in the creation and implementation of ISM policies. This will raise awareness among users and will allow developing policies that are more aligned with the users’ values and priorities. This will lead to policies that have better chances to be successfully adopted. It is equally important to be aware that regardless of the IT systems’ sophistication they have a very limited contribution in ISM without adequate behaviors and practices.
References


Leonardi, P. M. (2013). Theoretical foundations for the study of sociomateriality. Information and Organization, 23(2), 59-76.


