European Journal of Information Systems (2017) 26, 1–20

www.palgrave.com/journals

ETHNOGRAPHY/NARRATIVE

Information systems security policy implementation in practice: from best practices to situated practices

Elina Niemimaa[1] and Marko Niemimaa[2]

[1] *Department of Information Management and Logistics, Tampere University of Technology, Korkeakoulunkatu 10, 33720 Tampere, Finland;* [2] *Turku Centre for Computer Sciences/Information Systems Sciences, University of Turku, Turku, Finland*

Correspondence: Elina Niemimaa, Department of Information Management and Logistics, Tampere University of Technology, Korkeakoulunkatu 10, 33720 Tampere, Finland.
Tel: +358 406 8707 91;
E-mail: elina.niemimaa@gmail.com

Abstract
Organizations face institutional pressure to adopt information systems security (ISS) best practices to manage risks to their information assets. The literature shows that best practices should be contextualized, that is, translated from universal and general prescriptions into organizational documents and practices. Yet, little is known about how organizations actually make the translation from the best practices into situated practices. In this ethnographic study, we draw on practice theory and related concepts of canonical and non-canonical practices to analyze the process of translation. We explore how an IT service provider translated the ISS best practice of information classification into an ISS policy and into situated practices. We identify three translation mechanisms: (1) translating global to local, (2) disrupting and reconstructing local non-canonical practices, and (3) reconstructing and enacting local canonical practices. We find that while the translation was inhibited by incongruent practices, insufficient understanding of employees' work, and the ISS managers' lack of engagement in organizational practices, allowing situated practices to shape the ISS policy and actively engaging employees in the reconstruction of situated practices contributed positively to the translation. Contributions and implications for research and practice are discussed and conclusions are drawn.
European Journal of Information Systems (2017) **26**(1), 1–20.
doi:10.1057/s41303-016-0025-y; published online 9 January 2017

Keywords: IS security; IS security policy; practice theory; ethnography

Introduction

The cost of information systems security (ISS) breaches is ever-increasing (PWC, 2014). A recent industry survey reported that 76 percent of respondent organizations had already experienced or expected to experience a breach that resulted in (or would result in) the loss of customers or business partners (Ponemon Institute, 2013). In order to prevent such breaches and to respond to other ISS threats, organizations deploy ISS management (Smith *et al*, 2010). Organizations often follow the best practices outlined in ISS management standards, such as ISO/IEC27001, NIST-SP800, and PCI-DSS. Since ISS threats are constantly evolving, organizations increasingly face immense institutional pressures to adopt such practices and standards (Hsu *et al*, 2012). However, since the standards are universal and general in their scope (Siponen & Willison, 2009), they provide little guidance for organizations that wish to adopt them (Siponen, 2006). For example, the international ISS de jure standard

Editor: Frantz Rowe
Associate Editor: Michael David Myers

Received: 25 June 2015
Revised: 18 September 2016
Accepted: 29 September 2016

ISO/IEC27001 requires organizations to establish an ISS policy and suggests that the "set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties" (ISO/IEC, 2013a, p. 10). A related standard, ISO/IEC27002, provides implementation guidance for this requirement by specifying that the policy should "set out the organization's approach to managing its information security objectives" (ISO/IEC, 2013b, p. 2). Given the relatively high level of guidance provided by the standards on ISS best practices, many organizations face the challenge of understanding and translating the standards' requirements into something concrete and actionable. For example, in order to establish an ISS policy, most organizations must consider which practices should be included in the policy, why those practices should be included, how the requirements and practices in the policy should be justified and presented, and who should approve the new policy. When following the standard, organizations must further publish and communicate the policy and thus consider how, exactly, the policy should be implemented. Because policies are merely dead objects unless "they get situated in the flow of organizational life" (Ciborra, 1999, p. 86), ISS policies will only materialize in the enactments of situated practices in a given context (Niemimaa & Laaksonen, 2015). Organizations thus must consider how the communicated policy can be turned into employees' situated practices. At the same time, while ISS standards and best practices have received broad attention from scholars (Siponen, 2005; Siponen & Oinas-Kukkonen, 2007), translating the best practices into organizational practice has been of little concern in the existing literature.

Against this backdrop, this ethnographic study analyzes how ISS practitioners at an information technology (IT) service provider translated an ISS best practice of information classification into an organizational ISS policy and into local organizational practices. In doing so, the study draws on practice theory (e.g., Schatzki *et al*, 2001; Feldman & Orlikowski, 2011; Jarzabkowski *et al*, 2012) and the concepts of canonical and non-canonical practices (Brown & Duguid, 1991). Practice theory is a prominent analytical tool for analyzing and theorizing about contemporary management, as it is generally understood to be complex, dynamic, distributed, and emergent (Feldman & Orlikowski, 2011). It is particularly useful for understanding the interaction between institutional dynamics and local actions and vice versa (Smets *et al*, 2012), which in this study means the interaction between global ISS best practices and local actions.

The remainder of this paper is organized as follows. In the next section, we discuss the literature on ISS management, practices and policies, and introduce practice theory as well as the concept of translation. We then outline the research approach, after which we provide a description of the project we studied. We then analyze the ethnographic fieldwork and foreground the mechanisms of the translation from an ISS best practice to situated practices. Then, in the discussion section, we elaborate the findings of the study for ISS policy research and translation studies as well as for practice. Finally, we present our conclusions.

Theoretical background

Information systems security management and practices

While research has traditionally viewed ISS as a technical issue (Siponen & Oinas-Kukkonen, 2007), recently researchers and practitioners alike have argued that this view has significant limitations. For example, Straub *et al* (2008) argue that "the likely problem today is not the lack of technology, but its intelligent application" (p. 5). Likewise, Hsu *et al* (2012) suggest that "overall, information security is still in the primitive stages in terms of the management of information security rather than in terms of the extensiveness of security technologies adopted by organizations" (p. 920). Against this backdrop, researchers are increasingly interested in understanding ISS management. Central to ISS management is the use of ISS management standards such as ISO/IEC 27001, NIST-SP800, and PCI-DSS, as well as the best practices these standards prescribe. While standards are not the only method for implementing ISS management (e.g., benchmarking may be used), previous research highlights their importance and the benefits to organizational ISS (e.g., Von Solms, 1999; von Solms & von Solms, 2004; Saint-Germain, 2005; Siponen & Willison, 2009).

ISS management standards seek to be collections of ISS best practices (Ransbotham & Mitra, 2009) that are detached from actual practice through standardization processes (Backhouse *et al*, 2006) and that aim to be both authoritative and general (Siponen, 2005). Indeed, the current standards are bot universal and general in their scope (Siponen & Willison, 2009). For example, the controls specified in ISO/IEC 27002 "are acknowledged as best practices applicable to most organizations" (ISO/IEC, 2014, p. 17). Moreover, the standards have substantial authority among ISS practitioners, organizations, and governments. It is often claimed that they describe the "accepted" approach to organizational ISS, that they offer organizations a possibility of learning about successful ISS experiences of other organizations (von Solms & von Solms, 2004) and that adopting the best practices of a standard may help organizations in addressing different legal and contractual demands (Gerber & von Solms, 2008). Further, local governments may require organizations to comply with these standards (Smith *et al*, 2010). It is thus not surprising that organizations face institutional pressures to adopt both the standards and the practices that they prescribe (Hsu *et al*, 2012).

Researchers have studied ISS standard implementation projects. In particular, Smith *et al* (2010) investigated power relationships during a government-mandated ISS

standard implementation project within governmental agencies and Hsu (2009) analyzed how managers and employees made sense of a standard implementation project in a Taiwanese financial institution. While these studies do offer valuable insights into standard implementation, due to their level of analysis (i.e., standard implementation project), they do not attend to ISS practices or the ways in which certain practices are localized and become practiced locally in an organization. Hsu's (2009) study, however, demonstrates the importance of studying actual organizational practices, since her study shows how the management of a company perceived an ISS standard implementation project to be successful, yet it failed to bring about changes in actual practices. For example, the company's employees continued to use USB memory sticks, notwithstanding that this was against the ISS policy.

Implementing organizational ISS policies is a key ISS best practice (Baskerville & Siponen, 2002; Doherty *et al*, 2009). For example, the international ISS standard ISO/IEC27001 requires organizations to establish an ISS policy (ISO/IEC, 2013a) and ISO/IEC27002 recommends dozens of policies that organizations should implement (ISO/IEC, 2013b). Neither ISO/IEC27001 nor other standards address how ISS policy could or should be crafted in practice (Siponen, 2006). Indeed, there is a sense that "the details of practice have come to be seen as nonessential, unimportant, and easily developed once the relevant abstractions have been grasped" (Brown & Duguid 1991, p. 40). Despite the acknowledged importance, a literature review found that only 1.64 percent of 1280 articles surveyed could be categorized under the topic "security policies" (Siponen *et al*, 2008). In organizations, these policies must be crafted into material form by people (Coles-Kemp, 2009), by ISS practitioners. To this end, studies that focus on policy formulation often propose sets of high-level phases. For example, Whitman (2008) suggests the five phases of investigation, analysis, design, implementation, and maintenance and change. Similarly, Rees *et al* (2003) propose four major phases – assess, plan, deliver, and operate – each of which includes two discrete steps that are again divided into sub-steps that are executed in a sequence. Knapp *et al* (2009) suggest a repeatable flow of activities that consists of phases of risk assessment, policy development, policy approval, policy awareness and training, policy implementation, monitoring, policy enforcement, and policy review. Stahl *et al* (2012) question such policy creation by bringing to light the fundamental roles that ideology and hegemony may play in the process. Further, Dhillon *et al* (2007) challenge such phases by arguing that ISS policy implementation is likely not a set of discrete phases but an emergent process. As a result, Baskerville and Siponen (2002) argue that researchers should focus more on the implementation within empirical settings rather than on providing ready-made lists of particular actions that organizations should or should not do.

ISS policies highlight employees' roles and responsibilities in regard to information assets (Höne & Eloff, 2002) and document instructions as to what employees are expected to do when interacting with these assets (Whitman, 2008). Yet, the goals of ISS management can only be achieved if the policies and related procedures are complete, accurate, available, and eventually implemented (Warkentin & Johnston, 2008). To this end, scholars have examined employees' intentions to comply with the policies and have proposed different psychological antecedents of compliance (Warkentin & Willison, 2009). For example, formal and informal sanctions and penalties may influence employees' intentions to comply (e.g., Herath & Rao, 2009; Johnston & Warkentin, 2010). Further, neutralization may affect employees' intentions, as employees may rationalize their non-compliance (Siponen & Vance, 2010). Because compliance studies generally focus on employees' intentions and the underlying psychological factors, they do not attend to practices of compliance or organizational practices in which employees work. Yet, as the existence of compliance studies suggests, policies themselves are not enough, but the ISS practices they describe should be enacted in practice (Boss *et al*, 2009). Unfortunately, there is often a conflict in espoused theory and theory-in-use, that is, what is mandated in the policy is not translated into practice (Dhillon, 2007).

In conclusion, while previous studies have acknowledged the importance of best practices and standards for organizational ISS and research on standard implementation exists, studies on a different level of analysis, on implementing best practices locally, as required by the standards are few and far between. ISS practitioners face the challenge of turning best practices into organizational ISS policies and then turning those policies into practice.

Practice theory and canonical and non-canonical practices

Recent management and organization studies propose practice theory (e.g., Schatzki *et al*, 2001; Feldman & Orlikowski, 2011) as a useful approach for understanding the interaction between institutional dynamics and local actions and vice versa (Smets *et al*, 2012). Understanding the interaction links "what goes on deep inside organizations [with] … broader phenomena outside" (Whittington, 2006, p. 617). In this paper, that broader phenomenon is ISS best practices, while the organizational phenomenon is an organization's ISS practices. Practices are "arrays of activity" that are materially mediated and organized around shared practical understandings (Schatzki, 2001). The practice perspective thus implies research that focuses on people's recurrent everyday activities and on the enactments of organizational phenomena (Feldman & Orlikowski, 2011), such as an organization's ISS policies. The perspective also entails exploring what people in an organization actually do as opposed to what they aspire to do or what they or their

management say they do (Levina & Vaast, 2005; Orr, 2006; Suchman, 2007). The theory thus resonates with the recent elements of ISS research that have reinforced the idea that ISS practices only matter if and when they are enacted in practice (cf. Boss *et al*, 2009). Practice theory is widely used in a broad range of domains, including innovation (Dougherty, 2004), information systems (e.g., Orlikowski, 2000; Levina & Vaast, 2006; Arvidsson *et al*, 2014), and institutional change (Smets *et al*, 2012).

Central to practice theory is the notion that "social life is an ongoing production and thus emerges through people's recurrent actions" (Feldman & Orlikowski, 2011, p. 1240). The practice perspective thus entails an ontological reversal from an understanding of ISS practices as largely stable entities that describe specified roles and responsibilities for actors and activities – which change whenever a new ISS policy prescribes them to change – to an understanding of the continuous process through which these ISS practices emerge via enactment in practice. In other words, mere change in the descriptions of a policy will likely only decouple what organizations say they do from what they do. It is rather the implication of these policies in organizational practices that brings the documented practices into being and gives them definitive form and content (Niemimaa & Laaksonen, 2015). Acknowledging this perspective takes the individuals' actions seriously and addresses recent critiques that ISS standards focus on process and not content, and that better understanding of the emergent process of ISS policy implementation is needed.

Canonical and non-canonical practices In a seminal article, Brown and Duguid (1991) conceptualized organizational practices as canonical and non-canonical, thus differentiating described practices from what happens in practice. Canonical practices are the abstract, "thin" and formalized, and often directive descriptions of practices found in organizational documents. They usually assume a predictable and unproblematic reality and are therefore often ostensibly simple, and require interpretation in their use (Suchman, 2007). In contrast, non-canonical practices are situated, contingent, improvised, and often characterized by complexities, dilemmas, and a high degree of ambiguity. They are the specific actions taken by specific people at specific times when they engage in some organizational activity. In the context of ISS, non-canonical practices could be those improvised ones exemplified by Njenga and Brown (2012). Non-canonical practices may enact the canonical ones in multiple ways. Engaging in secure handling of classified information as defined in an organization's ISS policy, for example, may be substantially different for people in various organizational positions. Non-canonical practices always contain parts that are invisible and can never be rendered fully visible, and that are lost when standardizing and documenting those practices (Almklov & Antonsen, 2014). This implies that local performances of canonical practices need to be developed through situated engagement and application. More broadly speaking, ethnographic studies in management and organization studies illustrate the divergences between espoused practices and what actually happens; the latter usually differs from the ways research and organizations describe it in policies, standards, and the like (e.g., Orr 1996; Orr, 2006; Suchman, 2007). "It is the actual practices, however, that determine the success or failure of organizations." (Brown & Duguid 1991, p. 41). The same is arguably true for organizations' efforts to secure their information assets – organizational variance in their ISS performance is likely to emerge not from management prescriptions but from how those prescriptions *translate* to situated practices. We relate ISS standards and best practices to Brown and Duguid's (1991) canonical practices, since such practices are general, authoritative (Siponen, 2006), and documented descriptions of acontextual ISS practices. In a similar manner, ISS policies are documented, yet contextual descriptions of local ISS practices embed and reflect local management authority and expectations, and become included as part of organizational governance through formal acceptance procedures (including, for example, a signature from top management as a symbol of management acceptance and support (von Solms & von Solms, 2006)).

Translations in ISS policy implementation

Whereas canonical and non-canonical practices refer to abstract and situated practices respectively, translation is about the process whereby abstract practices are transformed and implemented in particular organizations. Our use of the concept of translation builds on ideas that originate from what Callon (2007) used to call the sociology of translation but that have been subsequently tailored to organization studies (Czarniawska & Joerges 1996; Czarniawska, 2004; Morris & Lancaster, 2006; Nicolini, 2010) and to information systems (IS) research (Nielsen *et al*, 2014). Translation differs from other types of interpretation and reproduction in that it both paraphrases and refers to its source (Hanks, 2014), but also because it always involves transformation (Czarniawska & Joerges 1996; Nielsen *et al*, 2014). Translation builds on the assumption that "a thing moved from one place to another cannot emerge unchanged: to set something in a new place or another point in time is to construct it anew" (Czarniawska, 2009, p. 425). In other words, the meaning of translation in this context far surpasses the linguistic interpretation, where translation would merely equate with substituting foreign words with their local equivalents (Czarniawska & Joerges 1996). As things travel across and within organizations, they undergo transformation. Translation is constrained by the target into which one translates (Hanks, 2014). For example, when ISS best practices are brought to a new organization, the contextual factors (e.g., organizational structure and culture (Karyda *et al*, 2005)) at the new organization constrain the possible ways in which those can be

implemented. Another key characteristic of translation is that it is not merely the things that become transformed, but translation modifies both "those who translated and that which is translated" (Czarniawska & Joerges 1996, p. 24).

These ideas of translation are emphasized in studies on the implementation of managerial practices (e.g., Powell *et al*, 2005; Morris & Lancaster, 2006; Nicolini, 2010; Nielsen *et al*, 2014). These studies have shown that, at the organizational field level, managerial practices, comparable with ISS best practices, transform as they become implemented and institutionalized locally as actors engage and transform the field-level ideas into locally practical use. When organizations translate practices into local practices, they are refined and modified, and some practices are privileged over others. For instance, in a recent study Nielsen *et al* (2014) showed how field-level ideas of possible IT use traveled across fields and within organizations and transformed, as they traveled, into different linguistic and material forms. Similarly, implementing ISS policies is not a straightforward and simple task of merely copying the best practices to local ISS policies, as the best practices must be contextualized to fit the local conditions (ISO/IEC, 2013a, b). Especially, fitting the abstract practices disembedded from other contexts to local conditions may prove difficult if the local and non-local practices are not sufficiently similar (Brown & Duguid, 2001). This is likely due to the fact that translation is rarely about words and more often about worlds (Leavitt, 2014).

For tracing the process of ISS policy implementation, translation offers analytical ideas of how the abstract descriptions of practices travel to specific contexts and become transformed as organizations seek to implement ISS policies and how those policies in turn become negotiated as meaningful and enactable in the context of their application. Abstract best practices are applied to a specific organizational context; they are iteratively and recursively transformed into local ISS policies, and the resulting policies may eventually disrupt and transform the local non-canonical practices. So far, theoretical foundations illustrate the importance and need for translating ISS best practices to situated practices and provide theoretical vocabulary for thinking through and organizing the decoupling between what is formally described of practices and what takes place in practice. However, an important gap on *how* the translation takes place remains (Morris & Lancaster, 2006). To analyze this, we now turn to our empirical materials.

Research approach

The analysis presented in this paper is based on an ethnographic study of developing and implementing an ISS policy at AlphaIT (a pseudonym), an IT service provider. An ethnographic approach attends to the particular context and is therefore suitable for a study that seeks to understand practices in a context: "Understanding actions and beliefs in their proper context provides the key to unravelling the unwritten rules and taken-for-granted assumptions in an organization" (Myers, 2009, p. 93). An ethnographic approach is one of the most in-depth research approaches available and is characterized by a researcher spending an extended period of time at the research site observing what people are doing as well as what they say they are doing (Myers 1999). Central to an ethnographic study is the sense of "being there," "being immersed in the situations, events, interactions and so forth" (Miettinen *et al*, 2009, p. 1315). Consequently, the ethnographic approach of this study affords potential for a deep understanding of the people, the organization, and the wider context. Moreover, ethnographic studies allow for building narratives that account for what happened, describe objects and argue about their relationships (Rowe, 2012). In short, quoting Ingold (2014), "In the conduct of our research, we [ethnographers] meet people. We talk with them, we ask them questions, we listen to their stories and we watch what they do. In so far as we are deemed competent and capable, we join in" (p. 386).

The project studied involved the development of a new information classification policy and several efforts to implement that policy. Developing and implementing such a policy presents a fruitful context for this study, as information classification policies represent a central ISS best practice, mandated by most ISS management standards (e.g., ISO/IEC27001, NIST-800, and PCI-DSS). For example, ISO/IEC27002 lists information classification as one of the core ISS controls (ISO/IEC, 2013b). The project was followed by the first author for six months in 2012 and 2013. During this time, she spent two to three days a week with the project team and participated in the project activities. This involved observing the practitioners in their work, attending meetings with them, and sharing informal situations such as lunch and coffee breaks with them. She conducted numerous informal discussions with them and reviewed the organization's ISS documentation. Last but not least, as a competent ISS practitioner, she participated in their practice, which gave her a genuine experience in ISS management (cf. Carlo *et al*, 2012) and a sense of being there (Myers, 1999). The participation of a researcher, being a participant observer, is beneficial for organizational ethnography, as it can enable the researcher to draw on experiences and the organizational members' responses in ways that might have been closed to researchers who are not participants (Van Marrewijk & Yanow, 2010). Accordingly, the empirical material primarily builds on participant observation of key actors involved in the project. Participant observation affords a detailed account of the work of individual employees (Davison *et al*, 2012), is crucial for analyzing practices (Schatzki, 2005) and provides the main source of empirical materials in ethnographic studies (Myers, 1999; Miettinen *et al*, 2009). Further, participant observations afforded us to be attentive to what the practitioners do rather than

what they or the management say they do. Additionally, follow-up visits of several days were conducted in 2013 and 2014 to observe the situation at the research site.

Data analysis proceeded in three steps. First, the first author wrote a rich chronological story of the development and implementation of the policy (Langley, 1999), employing a "thick" description mode of analysis (Geertz, 1973). The central analytical question here was *how* actors *do* the policy. Therefore, the concern was to longitudinally trace those actions that could be considered part of the development and implementation. This helped in the identification and description of key activities and events within the project. Second, the data analysis proceeded with intensive reading of the existing literature, story, and field notes as well as visualizing data in tables (Miles & Huberman, 1994). Through iterative reading of data and literature, the concepts *et al*of canonical and non-canonical practices (Brown & Duguid, 1991) emerged as partial explanations for what was happening at AlphaIT. Data, however, suggested a more granular division; the concepts of global canonical ISS practices, local canonical ISS practices, and local non-canonical ISS practices emerged from the data. Third, we analyzed the relationship between the uncovered canonical and non-canonical practices to understand how the abstract canonical practices were translated and performed by the actors. This analysis uncovered a series of interactive and reciprocal mechanisms in the relationship between the canonical and non-canonical practices. The three mechanisms were (1) translating global to local; (2) disrupting and reconstructing local non-canonical practices; and (3) enacting and reconstructing local canonical practices. The elements show how a global ISS practice became implicated in local descriptions of practices and eventually those became enacted in local practice. As a whole, this research approach is in line with prior IS research that draws on practice theory and ethnography (e.g., Jarzabkowski *et al*, 2012; Schultze & Orlikowski, 2004; Smets *et al*, 2012).

In the following section, an overview of the project studied is laid out as the social and historical context of the study (Klein & Myers, Klein and Myers 1999). In lieu of revealing the real name of the organization, we use a pseudonym and have anonymized all actors to preserve their privacy. We have translated notes and other written materials that were originally in Finnish to English.

Ethnographic description of ISS policy project

The context

AlphaIT provides IT services to several Finnish companies that have been classified as parts of society's critical infrastructure by the Finnish National Emergency Supply Agency. The services include information systems (IS) development and hosting for systems that process and store sensitive data [e.g., data that are regulated by privacy laws (see Warkentin *et al* 2011; Gillon *et al* 2011)]. The organizational culture values seasoned employees, hierarchical decision making, and in-depth knowledge of AlphaIT's long-standing customer strategy. Remarkable aspects of work include very stable responsibilities and an explicit and traditionally fixed division of work between management, those who work with IS and those who work with ISS. ISS is crucial for AlphaIT's business. Accordingly, AlphaIT has an ISS team led by a Chief Information Security Officer (CISO) and a separate, outsourced organization responsible for operational ISS. AlphaIT's ISS management has adopted different "guiding principles" for ISS and actively seeks guidance from best practices, such as ISO/IEC27001 and local standards. The CISO has just resigned, but a new one has already been hired.

The project

In 2012, AlphaIT requested an external ISS consultation company to assess the state of the company's ISS. This assessment resulted not only in appraisals of several aspects of AlphaIT's ISS, but also in a list of developmental recommendations. One of the most urgent recommendations concerned the existing ISS policy in general and its information classification policy section in particular. Referring to an ISS standard, the report suggested that the organization should adopt an ISS best practice of classifying information assets and handling information according to the information's classification. This practice was described in the standard with two general purpose statements and seven requirements. For example, one requirement was: "Employees know how to handle classified information." Thus both the report and the standard described the practice of information classification in a general and universal manner without explaining how the practice could be accomplished in any particular organization.

In late 2012, a project was initiated within AlphaIT to develop and implement a new information classification policy for handling classified information. Figure 1 depicts the project as a set of episodes and lists the main activities within each episode. From the beginning, the ISS professionals perceived the project as relatively straightforward and "business as usual." Thus the project was neither explicitly planned nor were the project objectives clearly defined. As was customary at AlphaIT, external consultants were given the responsibility to carry out the project. Initially, the core project team consisted of three consultants and AlphaIT's CIO: Peter, who had not consulted with AlphaIT before; Melissa, who had already been involved in previous ISS policy development initiatives; Sven, who had been involved in the aforementioned assessment; and Paul, the CIO. Later, the new CISO, Julia, became part of the team and the CIO stepped aside.

In November 2012, Peter reviewed the existing information classification policy. Drawing on his general ISS experience, he crafted a new policy and related guidelines for handling classified information based on "common

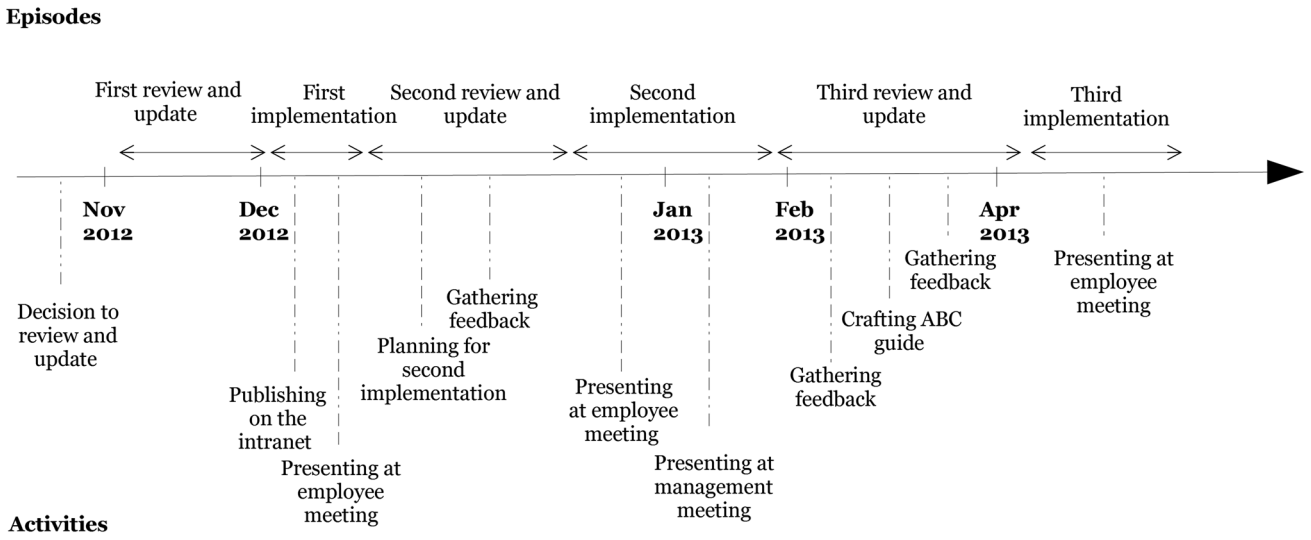

Figure 1 Chronology of project episodes and activities.

ISS knowledge," as he called it. The policy and guidelines described the purpose of information classification, related roles and responsibilities and a set of practices for handling information. After this initial review and update, the three consultants sat down for a workshop to review the policy and to ensure it reflected AlphaIT's business. According to them, the policy was written to convey information to employees about the expected ways employees should work in regard to information classification. It had to be sufficiently general to cover different situations and events, and it was not designed to explain or provide guidance for employees. The accompanying guidelines offered simple examples of actions expected from employees in a few sample situations of classifying and handling information. At the same time, AlphaIT recruited a new CISO. She soon decided that the review and update was complete, but with minimum effort and without workshops or interviewing AlphaIT's employees. She further stated that the policy was in line with her ambition to transfer much of the burden of securing AlphaIT's IS from ISS professionals to system owners and operations managers. First efforts to implement the policy were not explicitly planned. Neither the consultants nor the CISO anticipated any issues in regard to the implementation; they assumed that employees would be able to follow the policy after it had been introduced to them without requiring significant know-how or understanding. The ISS professionals did not think that the policy would espouse large changes in the behavior of AlphaIT's employees or affect its business or customers. The CISO simply published the policy in AlphaIT's Intranet and presented it in an employee meeting. To her great surprise, the policy was received with crushing feedback. Employees argued against the policy and pointed out several difficulties it would introduce to their work and for AlphaIT as a company. Meeting participants agreed that the policy had to be refined and employee feedback addressed. Employees continued their normal work without considering the information classification.

Refinements and new implementation efforts followed. The CISO asked Sven to work on the policy with selected employees to address employees' views and to plan for a reimplementation effort. While Sven had participated in the workshop mentioned above, he was not familiar with the finalized version of the policy. He spent time reading and comprehending the intent of the policy and the expected effect on employee behavior. In contrast to his expectations at the beginning of the project, the expected changes were multifaceted. Despite his relatively long career as an ISS management consultant, Sven was not familiar with ISS campaigns nor did he have practical experience with other implementation methods. He searched for materials and inspiration from the Internet [e.g., materials from European Network and Information Security Agency (ENISA)] about campaigns as a means for implementation. He planned a step-by-step implementation that included a poster and email campaign and presentations in employee meetings and in meetings where representatives of AlphaIT's customers were present. In parallel with planning the implementation, Sven invited key system owners and operations managers into separate meetings to share their views on the policy. System owners and operation managers commented on every sentence, sometimes every word, written in the policy. Many of the problematic sentences they brought up were related to AlphaIT's long-standing relationship with its customers. They were further reluctant to embark on the new responsibilities the policy would place on them. They stated that they were afraid that those would increase their workload. They also indicated that they did not possess the required knowledge of ISS to assume the

responsibilities. Reflecting the organization's culture of a strict and fixed division of work tasks, they saw ISS as the CISO's responsibility, not theirs. The CISO and the consultants were surprised to hear these views expressed. Only at this point did they realize that the concept of information classification and the related practices were new to most of the employees. To ISS professionals such as themselves, the classification was a normal part of work in almost any business.

After slight changes to the policy, it was implemented for the second time; Sven introduced the changes in an employee meeting and the changes were received with a series of questions. Employees appealed to the organization's customers and stated several times that the data, stored in AlphaIT's IS, are owned by their customers, not by AlphaIT or its employees. Therefore, they saw that the role of "information owner" (i.e., one of the roles in the policy) was inappropriate. In their view, none of them could assume the role, as they did not own the information and could not therefore be responsible for it. They further seemed to agree that they could not take the responsibility over security of the IS, as they did not have the required knowledge of ISS and further because they did not know how AlphaIT's customers required the information to be protected. On the other hand, AlphaIT's customers relied on its ability to secure their information. In addition to the employee meeting, the CISO introduced the policy to AlphaIT's management group. According to her, group members did not generally understand why the organization needed information classification.

The management group decided that the policy and the guidelines had to be augmented with a more practical "ABC Guide to Information Classification" that would explain, in simple terms, the intent of the classification and how it should be applied in everyday work. The CISO asked Sven to discuss it with system owners and one operations manager in order to develop practical examples of how classification could be applied in their work. Again, Sven browsed the Internet to gather ideas for the ABC guide and to craft a PowerPoint presentation that would serve as the ABC guide. He invited four system owners, of which two agreed, to have a small workshop with him to develop the method for classifying IS documentation in accordance with the information classification policy. This was selected as a topic of the workshop, as it was closely related to system owners' daily work. After the workshop, the participating system owners started to ask questions of the ISS professionals about information classification via email and informed their teams about the classification.

The implementation of the information classification received unexpected support from AlphaIT's decision to outsource parts of its IS development overseas. As information stored in AlphaIT's IS was regulated by privacy laws, the decision meant increased management interest in AlphaIT's ISS and, in particular, to information classification. Management demanded that the ABC guide be presented to AlphaIT's employees as soon as possible. They further required that feedback to the ABC guide must be gathered from all the system owners' managers and the guide be adjusted according to their feedback. The CISO asked Sven to send the ABC guide to all the system owners' managers for a review. Thereafter, Sven refined the ABC guide PowerPoint presentation with the information he had gathered during the workshop and sent it to managers. He received only minimal feedback, but modified the presentation accordingly.

It was not until a half year after the decision had been made to review and update the information classification that the classification policy, the guidelines, and the ABC guide were presented in an employee meeting with only minimal feedback. Soon after, employees responsible for customer communications included information classification in the related formal process descriptions and employees responsible for supply contracts sought to include the information classification requirements in contracts made with suppliers. The ISS professionals soon documented their efforts to the organization's procurement procedures and sought to make information classification an established practice with AlphaIT's suppliers. Nevertheless, the CISO and the consultants were tired and frustrated and wanted to forget all about information classification. They concluded that the implementation was finalized and they should proceed with other topics.

Later site visits showed that while the ISS professionals made no further explicit implementation efforts, employees had begun to enact the policy. Some employees were involved in the outsourcing project and thereby began to understand the requirements for protecting information. They seemed to seek guidance for meeting the requirements of the policy and distributed it and the related guidelines to their outsourced teams. Management requested that a placeholder for information classification be included in document templates and the Intranet configured to ask for the classification for all uploaded information. The ISS professionals received more and more emails asking about the classification and its application in employees' work.

Translating a global ISS practice to situated practices

Our empirical materials suggest an iterative and reciprocal translation from the prescriptions of an ISS best practice into situated practices, as illustrated in Figure 2. In this section, we elaborate the translation. The following analysis concentrates on the three uncovered types of interrelated strata of ISS practices and their interplay during the policy crafting and implementation at AlphaIT: (1) global canonical ISS practices, (2) local canonical ISS practices, and (3) local non-canonical ISS practices. "Global canonical ISS practices" refer to best practices for managing ISS as they are inscribed programs of actions (Hanseth & Monteiro, 1997), abstracted from

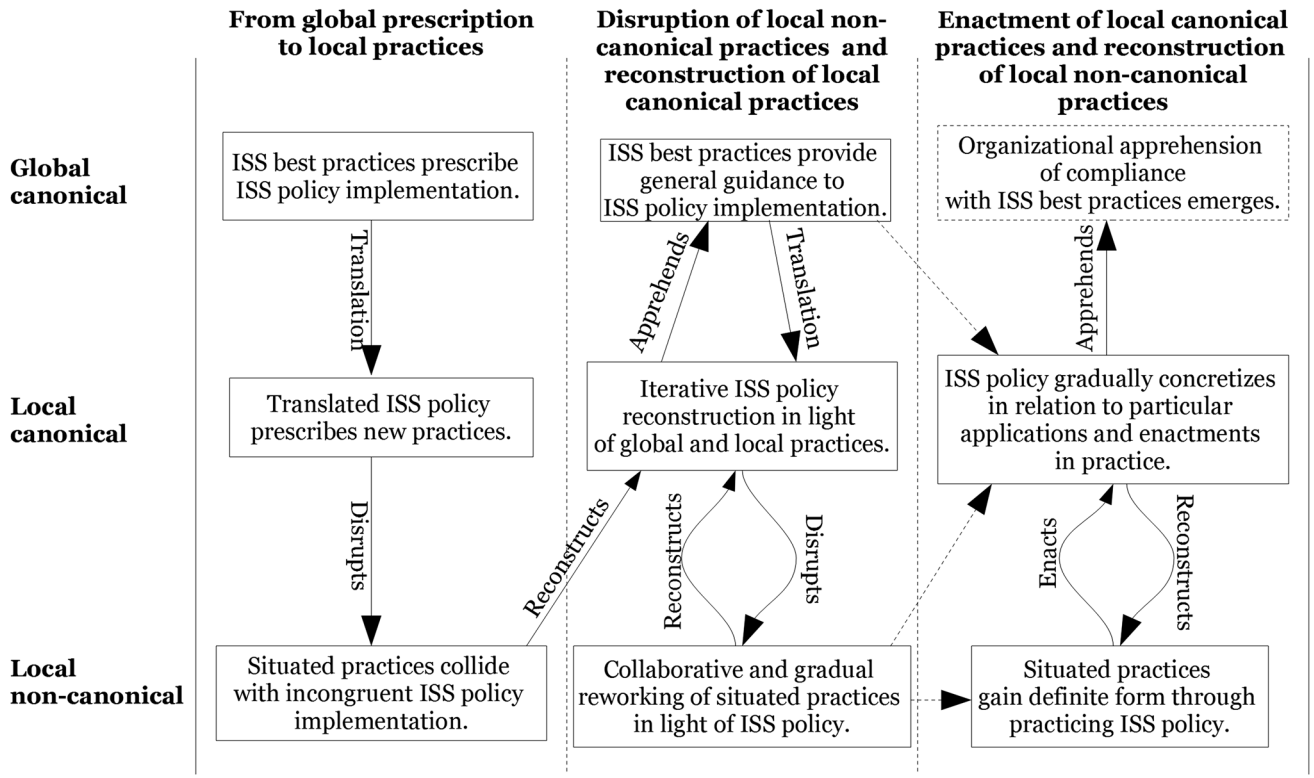

Figure 2 ISS policy implementation at AlphaIT.

local practice through standardization processes (Backhouse *et al*, 2006). They are global in scope, general and authoritative in style and form an institutionally approved corpus of requirements. For AlphaIT, the best practices posed authoritative requirements whose authority and guidance were not explicitly or directly confronted. "Local canonical ISS practices" are organization's descriptions of its ISS practices, such as policies and guidelines. For AlphaIT, they were "canonical" in that they documented management expectations, were included in the corpus of organizational documents and were formally approved. In contrast to descriptions of practices, "local non-canonical ISS practices" are situated practices; it is what happens in practice. In short, best practices are acontextual, ISS policies are contextual and local practices are enacted.

Translating global to local

A global canonical ISS practice became articulated in AlphaIT's descriptions of its ISS practices through situated actions that enacted some of its elements. This consisted of actions necessary for understanding the abstractions of the global practice locally and actions that translated it into a description of a local practice. The ISS professionals at AlphaIT faced institutional pressures to adopt the global ISS practice (Hsu *et al*, 2012) of classifying information assets both as policy and in practice. The existing information classification policy had been left untouched by the employees; it existed in the Intranet but was never translated into actions, as employees did not enact it in their situated practices. It remained as a management description of what employees do, which was disconnected from what they actually did, as a canonical practice and not as a non-canonical practice. The issue for the ISS professionals became that of understanding and enacting such a global canonical practice in practice. They had to make something particular from the abstract and universal descriptions provided in the ISS standards. In so doing, they relied on their knowledge of ISS standards and other best practices and on their experience and skills in crafting ISS policies to translate the global practice into a local one. Without involving other employees, they translated the requirement of establishing an information classification into a policy document that first described the purpose of information classification in abstract and general terms and then stated a bundle of descriptions of new local canonical ISS practices that prescribed organizational expectations for employees when handling organization's information assets. Employees were expected to unambiguously understand the concepts in the policy and guidelines, and to be able to easily assume the prescribed practices in their work tasks. Employees were expected to follow the policy and guidelines without requiring significant know-how or understanding. Table 1 illustrates the translation and implications for situated practices.

Disrupting non-canonical practices and reconstructing canonical practices

At AlphaIT, ISS professionals sought to disrupt employees' situated practices and complement or modify them with the canonical practices documented in the new policy. This was characterized by actions that introduced the new canonical practices to organizational members and, by so doing, tried to break the existing patterns of recurrent practices. For example, the CISO and the ISS professionals published the policy and guidelines in the Intranet and introduced them in employee and management meetings. After the policy was introduced, the discussions at AlphaIT were marked by a clash of prevailing organizational practices and the introduced ISS practices. By enacting the practices of her previous workplace, the CISO had decided to accomplish the project with minimum effort and without involving AlphaIT's employees and had commenced to publish the policy and present it in an employee meeting. Yet, employee involvement and rigorous reviews of all new organizational documents were established organizational practices embodied in routines and operating procedures of AlphaIT. These organizational practices subtly shaped employees' expectations and behavior in regard to the implementation of the information classification policy; for them, review and involvement before implementation were self-evident. Consequently, the prevailing organizational practices and the way a new ISS practice was introduced were incongruent. As such, the first introduction raised more discussions than it broke the existing patterns of recurrent practices. The discussions and crushing feedback resulted in a decision to modify the policy. The non-canonical local practice had hit back. Introducing the policy had not resulted in the reconstruction of the employees' practices, but they continued to reinforce the existing practice.

Further incongruence between the described practices of the policy and the actual practice surfaced in the workshops Sven, one of the consultants, arranged (Table 2). Those were related to AlphaIT's long-standing strategy for its customer relationships, current employee responsibilities and their perceived lack of skills and know-how in issues pertaining to ISS. The strategy of customer relationships implied that ISS was not seen as a business network-level issue but was regarded as each organization's private concern. The local mode of managing ISS at AlphaIT entailed that the ISS professionals alone were responsible for AlphaIT's ISS. Previously, all tasks that could be interpreted as ISS related had been given to the ISS professionals. Thus, the employees had not assumed any ISS responsibilities. This state of affairs legitimated employees' claims for lack of skills and know-how and, by opposing new responsibilities, they reinforced the prevailing practice. The mode of managing ISS further meant that the ISS professionals were not involved in the tasks other organizational members performed. Consequently, there was a gulf between the ISS professionals' practices and that of the rest of the organization.

Table 1 Examples of translating global canonical practices to local canonical practices

Global canonical ISS practice	*Local canonical ISS practice*	*Situated practices*
Employees know how to handle classified information	Each employee is responsible for securing AlphaIT's information assets. Each employee must ensure that he or she handles information according to the policy and ascertains the security of information	Neither existing nor new policy was enacted in practice. Information classification was not reflected in employees' work
When no longer necessary, information is destroyed using methods that ensure confidentiality and privacy	Disposal of public information is not restricted. Medium where internal or confidential information is stored should be disposed by using secure containers	

Table 2 Examples of incongruence in canonical and non-canonical practices

Local canonical ISS practice	*Situated practices*
All information assets must have an information owner. Owner must be AlphaIT's employee	In situated practices, AlphaIT's customers were solely responsible for the information processed in AlphaIT's IS. AlphaIT provided them with IS and related processes
Information owner is responsible for the information including, among other things, classification of information and compliance to privacy laws. For confidential information, owner is responsible for the security level of the IS where information is processed	ISS professionals were responsible for AlphaIT's ISS and conducted all tasks related to ISS. Employees did not assume any responsibilities for securing information or IS. AlphaIT had strict and fixed divisions of work tasks
Disposal of public information is not restricted. Medium where internal or confidential information is stored should be disposed by using secure containers	Public, internal and confidential information was disposed customarily to a normal recycling bin. Secure containers were not available in all office spaces

Viewing this through a practice lens emphasizes that it is through engagement in the "doing" that such incongruence comes to the surface. The ISS professionals had to reconstruct the policy in the light of the incongruent practices. Yet, the same issues of customer relationships, defined roles and responsibilities, and skills arose again in an employee meeting where Sven presented the modified policy. The changes made and new implementation were not enough to break the existing patterns of practices, as the policy still contained elements that were in conflict with employees' work and skills. Having to think of "ISS roles and responsibilities differently" introduced a complexity to employees' everyday practices that revealed a mutual lack of understanding between the employees and the ISS professionals. Whereas employees complained that they had neither the time nor the skills to adopt the responsibilities, the ISS professionals, reflecting global ISS practices, held the view that those responsibilities were self-evidently the employees'.

Again, the non-canonical practice reconstructed the canonical practice as AlphaIT's management sought a solution from more detailed guidelines; a more comprehensible and usable description of the espoused practices of the policy was expected to suffice. In order to construct more detailed guidelines and to modify the policy, Sven sought help from global canonical ISS practices. Drawing on these practices, he presented information classification as a figure and wrote the ABC guide around the figure. He further convened workshops to categorize IS documentation according to information classification. The workshops and the making of the ABC guide illustrated that the ways employees worked and could apply the classification to practice were observably different from the ways it could be described in the policy. Even very simplistic situations, such as categorizing IS documentation, fell outside the guiding policy and crafted guidelines that tied categorization to abstract definitions of "information owner" and "information user" – obscure to employees. As information classification as a practice was new to most employees, it further fell outside their accumulated experience. As such, more and more detailed canonical practices would not suffice; the ISS professionals would not be able to document each and every situation where classification could be applied; all work related to it could not be anticipated completely in advance. Nevertheless, introducing the policy repeatedly and disrupting current practices slowly changed the current practice and came to reconstruct the policy; the iterative reconstruction of ISS policies and situated practices gradually reworked both the policy and practice. The incongruence that surfaced between the canonical and non-canonical practices was a driving force for the reconstruction of the local canonical practice in order to make it suitable and enactable to the organization (Table 3). In this way, non-canonical practice reconstructed the canonical one. At AlphaIT, the ISS professionals rewrote the policy and guideline several times.

Enacting canonical practices and reconstructing non-canonical practices

The local canonical practices became enacted by organizational members when they broke the existing pattern of local non-canonical practices and reconstructed them. This required that organizational members learned what the introduced practice was, as it is part of the nature of a practice "that learning what it is and enacting it are inseparable" (Barnes 2001, p. 33). In other words, a change in ISS behavior of organizational members was only possible when they learned the practice, discontinued reinforcing the old practice, and reconstructed a new one by enacting the canonical practice or some of its elements. At AlphaIT, motivated by the sudden legal pressures introduced by the overseas outsourcing of IT systems and enabled by a growing awareness and understanding of information classification practices, employees became more active and asked more questions of the ISS professionals about the classification. They even seemed somewhat proud when they remembered to classify information. Further, employees began to inform the ISS professionals about occasions where they had

Table 3 Examples of local non-canonical practices reconstructing canonical practices

Original local canonical ISS practice	*Reconstructed local canonical ISS practice*
All information assets must have an information owner. Owner must be AlphaIT's employee	Customer information explicitly separated from AlphaIT's information. All AlphaIT's information must have an information owner Contact email address was provided for information owners for asking questions about information classification
Information owner is responsible for the information including, among other things, classification of information and compliance to privacy laws. For confidential information, owner is responsible for the security level of the IS where information is processed	Information owner is responsible for the information including, among other things, classification of information and compliance to privacy laws. For confidential information, owner is responsible for the security level of the IS where information is processed Information custodian is responsible for IS and its ISS as instructed by the information owner of the information processed in the IS. The CISO is responsible for actively supporting information custodians
Disposal of public information is not restricted. Medium where internal or confidential information is stored should be disposed by using secure containers	Disposal of public information is not restricted. Medium (such as USB memory stick or paper copy) where internal or confidential information is stored should be disposed by using secure containers

witnessed someone disposing of classified information in a normal recycling bin; something prohibited by the new policy. Many enacted the policy by categorizing and disposing information according to its classification. In using the categorized information, they acted more freely and diverged from the canonical practice outlined in the policy, as most situations they encountered were not described per se in the ISS policy or related guidelines. Actual practice seemed to be anything but a simple following of the canonical practices. Only through its application and enactment in various situations, the ISS policy began to gain its definite content – the practices documented in the policy gradually concretized. The same also seemed to apply vice versa. The situated practices gained their definite form only in relation to the ISS policy. Thus it seemed the local situated practices only acquired definite form, and ISS policies acquired definite content, together. In other words, the canonical practices and non-canonical practices mutually constructed the information classification practices of AlphaIT.

In summary, the empirical materials of this study suggest how a translation from a global canonical ISS practice to situated practices happened at AlphaIT. The global ISS practice of information classification became articulated in AlphaIT's ISS policy through situated actions that understood and translated it. Introducing the new local canonical practices collided with local non-canonical practices that highlighted the incongruence in those practices. The foregrounded incongruence became a crucial driving force for the translation from a global to local practice, as it became the focus of reconstructing the local canonical practice in order to make it enactable by the employees. In this way, the non-canonical practice reconstructed the canonical one. The local canonical practices became enacted by organizational members when they broke the existing pattern of local non-canonical practice and reconstructed it. Moreover, there was an iterative relation between the global canonical practice, local canonical practice, and local non-canonical practice such that the translation happened through practices iteratively constructing and constituting each other. Thus what resulted as the implemented ISS policy was neither the best practices nor the organizational situated practices, but was co-constituted and co-created by both. It was, further, an emergent organizational understanding of compliance to an international ISS standard.

Discussion

Drawing on the practice theory (e.g., Schatzki *et al*, 2001; Feldman and Orlikowski, 2011) and the concepts of canonical and non-canonical practices (Brown & Duguid, 1991), this study sought to improve our understanding of the process of how prescriptions of global ISS best practices become situated practice. In particular, the study analyzed how the ISS best practice of information classification was translated into organizational ISS policy and situated practices. We contribute to literature on ISS policy implementation and on translations in management practice implementation.

As indicated in Figure 2, the study suggests that the prescriptions of a global ISS practice became implicated in situated practice through a translation whereby the prescriptions were translated into an organizational ISS policy, the policy disrupted and reconstructed situated practices, and the situated practices reconstructed and enacted the policy. The translation was inhibited by incongruent practices, insufficient understanding of employees' work, and the lack of the ISS professionals' engagement in organizational practices. Translating the ISS best practice into organizational ISS policy, allowing organizational practices to modify the policy and reconstruction of new situated practices by employees contributed positively to the translation. The primary findings are summarized in Table 4 and their implications are discussed below.

Implications for the ISS policy implementation literature

While ISS standards are important for organizational ISS (e.g., von Solms, 1999; von Solms & von Solms, 2004; Saint-Germain, 2005; Siponen & Willison, 2009), they have been argued to prescribe universal or general practices without giving sufficient attention to the organizational differences (Siponen & Willison, 2009) or to the content of those practices in organizations (Siponen, 2006). In other words, as collections of canonical practices, they "inevitably and intentionally omit the details" (Brown & Duguid, 1991, p. 40), making them too abstract to be directly applicable to a specific organizational context. Finding 1 (Table 4) provides empirical support to these previously conceptual arguments. It further contributes to literature by suggesting that a translation from the best practice to an organizational ISS policy and to situated practice is needed and accomplished by identifying the mechanisms of such a translation. As canonical practices, the prescriptions of the ISS best practice of information classification were necessarily incomplete and insufficient for local action. They offered ISS practitioners what Suchman (2007) would call "a plan," but, as analysis in this study illustrated, the plan fell short of the complexity of actual organizational life. The ISS professionals had to translate the abstract and universal prescriptions into an organizational ISS policy, which required interpolations between the abstract account of the global canonical practice and the situated demands. Accordingly, the ISS best practice provided a direction and an understanding *which* ISS practices AlphaIT should deploy, but AlphaIT had to boil down and concretize the requirements sufficiently in order to formulate local ISS practices.

Table 4 Summary of findings and their relation to existing ISS research

Finding	*Previous findings and new contributions to ISS research*
1. ISS best practice should become translated into organizational ISS policy and implicated in situated practice	This finding supports previous conceptual claims that the ISS standards provide too general and abstract guidance to organizations (Siponen, 2006; Siponen & Willison, 2009). This study adds to previous studies that to translate ISS best practices is to boil down and concretize the abstract ideas sufficiently to be practically useful and enactable in a given context
2. ISS policy should become congruent with the organizational (non-canonical) practices	This finding is new in the area of ISS policies and extends previous research that recommends what ISS policy should contain (Höne & Eloff, 2002; Whitman, 2008) to what the policy should be
3. In order to arrive at an ISS policy that is congruent with organizational practice, organizational practice should be allowed to reconstruct the policy 4. In order to arrive at an ISS policy that is congruent with organizational practice, ISS practitioners should engage in the "doing" of employees' work	These two findings answer calls from the literature for an improved understanding of the emergent process of policy implementation (Baskerville & Siponen, 2002; Dhillon *et al*, 2007) and challenge the authoritarian approaches (cf. Stahl *et al*, 2012). Findings extend previous research on the gulf between ISS managers and employees (Albrechtsen & Hovden, 2009; Niemimaa *et al*, 2013) with an empirical example on how the gulf could be narrowed in practice
5. ISS policy should disrupt and reconstruct prevailing organizational practice	This finding adds to ISS policy implementation by highlighting that, as introducing any new practices takes place in an existing organizational context (Karyda *et al*, 2005), the introduction of the practices requires not only situating those practices as part of the existing flow of organizational practices, but also transforming the existing practices. As such, to comply with the implemented ISS policies is not merely about intentions (e.g., Herath & Rao, 2009; Myyry *et al*, 2009; Warkentin *et al*, 2011; Johnston *et al*, 2015) or about adopting *new* practices but about integrating and relating those new practices to the existing work patterns, which always requires transforming the old
6. Enacting ISS policy requires that employees learn the policy's practices, break the existing pattern of practices and reconstruct new non-canonical practices	This finding offers new insights into ISS training (D'Arcy *et al*, 2009; Puhakainen & Siponen, 2010; Karjalainen & Siponen, 2011) by illustrating the situated nature of learning and to ISS policy implementation literature (e.g., Karyda *et al*, 2005; Kolkowska & Dhillon, 2013) by showing that employees translate and transform ISS policies as they reconstruct their existing work and practices. These contributions highlight employees as active actors in ISS management (cf. Bulgurcu *et al*, 2010; Niemimaa & Laaksonen, 2015) rather than as "enemies" (see also Hedström *et al*, 2011)

Finding 2 suggests what the ISS policy should be like – congruent with organizational, non-canonical practices. The finding is, to the best of our knowledge, new in the area of ISS policies. Incongruence between ISS policy's practices and the organizational practices (e.g., how employees accomplish their work) inhibited the translation from the best practice to situated practice. At first glance, the collision of practices may appear as employee resistance toward the ISS policy, but, more than resistance, it may be a signal that employees are unable to enact the practices documented in the policy in their work. Enacting the documented practice would, for example, impede their work or prevent them from achieving their work goals. Previously, ethnographic management studies have indeed found that incongruence between espoused practices and situated practices makes work difficult to accomplish (Orr, 1996). Finding 2 highlights a starting point for translating the ISS best practice into organizational ISS policy: it should be the organizational practices and the local ways of working. Therefore, policy should not only document instructions as to what employees are expected to do when interacting with the organization's information assets (Whitman, 2008), but the instructions should be such that employees can draw upon them as a set of resources in the course of their work.

Findings 3 and 4 relate to the formulation of an ISS policy. While previous research proposes general and abstract phases for policy formulation (Rees *et al*, 2003; Whitman, 2008; Knapp *et al*, 2009), more understanding of its emergent process has been called for (Baskerville & Siponen, 2002; Dhillon *et al*, 2007). Finding 3 answers these calls from the literature by detailing that the organization's non-canonical practices reconstructed the ISS policy throughout the policy formulation and implementation. The temporal emergence of the policy was the result of its incorporation into the existing practices and its modifications in response to the issues

encountered in implementing the policy. As such, the finding demonstrates the centrality of the existing local non-canonical practices in shaping the descriptions of local canonical practices (e.g., ISS policies). It shows that the canonical practices are not fixed but continuously produced and reproduced as they are enacted in practice. Thus policy and what happens in practice are mutually implicated in each other's creation. At AlphaIT, while the first version was crafted by the ISS professionals, the organizational actors began to enact it only after changes emerged from organizational practice. Therefore, the finding challenges the authoritarian approach to ISS policy formulation (Stahl *et al*, 2012), where the ISS policy is imposed upon, rather than negotiated with, the employees, by suggesting that an organization – its existing practices – should shape the ISS policy. Doing so requires not only proficiency in ISS practices, but also underlines the importance of understanding the employees' work and the local ways of working. This requires ISS professionals' active engagement with the employees' work (Finding 4), and vice versa.

Previous research indicates that an ISS digital divide may exist between ISS managers and employees (Albrechtsen & Hovden, 2009) and that incongruence in ISS managers' and employees' frames of reference may lead to ISS policies that are unacceptable for the employees (Niemimaa *et al*, 2013). As the ethnographic description of the present study illustrates, the ISS professionals' view of employees' work can overlook and sometimes oppose what it takes to get employees' work done. Finding 4 contributes to literature by suggesting a way forward: ISS managers should engage in the "doing" of employees' work in order to translate the requirements of a best practice into an ISS policy that is congruent with organizational practices. Insufficient understanding and accommodation of local ways of working initially led to an ISS policy that employees could not enact in practice (see Finding 2). Such a situation may enforce employees to violate the ISS policy in order to keep up with their work (Siponen & Iivari, 2006). Viewing this challenge from a practice perspective highlights that it is through engagement in the "doing" of work that incongruence and incompatibilities in described practices and actual practice become problematized and the gulf between the ISS managers' and employees' understanding is bridged.

Inscriptions of standards are only as useful as they actually succeed in making a change in organizational behavior (Hanseth & Monteiro, 1997). That is, local actions and practices are what make the difference in an organization's efforts to secure their information assets. A number of ISS policy compliance studies base their theorizing on the assumption that changing employee behavior is difficult (e.g., Herath & Rao, 2009; Warkentin *et al*, 2011; Johnston *et al*, 2015). This study provides empirical support for these claims and, as a new contribution, suggests that the change requires that ISS policy disrupt and reconstruct the prevailing organizational practice (Finding 5). Thus, in contrast to the existing accounts that locate the needed change in employees' intentions (e.g., Herath & Rao, 2009; Myyry *et al*, 2009; Warkentin *et al*, 2011; Johnston *et al*, 2015), this practice perspective-based study casts the needed change in organizational practices. At AlphaIT, for example, the needed change implied employees broke the existing organizational practices related to information classification and began to categorize and dispose information according to the new policy, which necessitated the employees to change their existing work patterns. Indeed, from the practice perspective, a change, even an institutional change, originates in an ordinary, everyday "doing" and work of people (Smets *et al*, 2012). Similarly, the change at AlphaIT originated from seemingly mundane actions: disposing classified information to a secure container, avoiding confidential discussion in public office spaces, and marking documents with confidentiality marks. Further, in line with recent studies on ISS awareness (Tsohou *et al*, 2012, 2015), disrupting the local non-canonical practice (i.e., how people work) is an active engagement of the various actors required for reconstructing that practice.

Finding 6 provides more depth to finding 5 by highlighting what is required for employees to enact a new practice: they have to learn the ISS policy's practices, break the existing patterns of their practices, and reconstruct new non-canonical practices. Due to the nature of canonical practices, ISS policies can never document each and every situation that employees encounter in their work and ISS policies always require interpretation in their use (cf. Suchman, 2007). This study illustrated how an ISS policy was exhausted in practice when it faced the complexities and unpredictability of everyday work. The invisible aspects of local situated practices not present in descriptions of "standardized" practices (Almklov & Antonsen, 2014) need to be locally developed through enactment of the ISS policy. Therefore, employees have to make complex interpolations and sometimes improvisations from policy to practice. Such interpolations and improvisations highlight the need for new theories for ISS policies that guide employees in such situations. Here, design theories proposed by Siponen and Iivari (2006) may prove helpful. For example, it may be useful to document key actions expected from employees in the ISS policy and allow them otherwise follow their intuition [i.e., the "liberal-intuitive design theory" discusses in Siponen & Iivari (2006)]. Yet, as the required interpolations and improvisations illustrated by this study show, listing all actions expected from employees in all situations (i.e., the "conservative-deontological design theory" discussed in Siponen & Iivari (2006)) is likely not feasible. At the same time, the interpolations and improvisations illustrate a basic tenet of the practice perspective: enacting a practice is inseparable from learning it, and the more the practice is enacted, the better participants become at the practice (Barnes, 2001). This suggests new insights into ISS training literature (D'Arcy *et al*, 2009; Puhakainen & Siponen, 2010; Karjalainen & Siponen,

2011) and into more general literature on ISS policy implementation (Karyda *et al*, 2005; Kolkowska & Dhillon, 2013). For the ISS training literature, it adds that learning largely happens in situ. By implication, therefore, training approaches that strip away context should be examined with caution and approaches that build upon authentic work practices should be fostered (Brown & Duguid, 1991). Further, while instructed classroom ISS training seems to abound in the literature (see Karjalainen & Siponen (2011) for a review) and training mostly focuses on routine work processes (Puhakainen & Siponen, 2010), the situated nature of learning and the interpolations required by unexpected situations call for complementary approaches to ISS training, approaches that do not isolate learning from employees' practice. For ISS policy implementation literature, finding 6 emphasizes the active role of employees in policy implementation. As non-canonical practice is an ongoing production and emerges from people's recurrent actions (Feldman & Orlikowski, 2011), the employees are required to break the existing pattern of practices and reconstruct new ones. At AlphaIT, policy implementation was not considered successful before employees had contributed to the policy and altered their practices. Prior implementation efforts were in vain as employees were not involved and, as such, their practices remain unchanged. Policy materializes differently in different enactments (Niemimaa & Laaksonen, 2015). Consequently, this study emphasizes the role of employees in ISS management.

The concepts of canonical and non-canonical practices arose as partial explanations when we sought to understand what was happening in an empirical setting. In particular, they provided us an insight into an issue that ISS literature notes as a problem but for which it does not afford concepts: how an ISS best practice becomes situated practice. Whereas canonical practices are characterized by abstract and "thin" descriptions, non-canonical practices are situated and characterized by complexities, dilemmas, and a high degree of ambiguity (Brown & Duguid, 1991). ISS best practices embody the characteristics of canonical practices. Highlighting that canonical and non-canonical practices are qualitatively different suggests that a translation is needed in moving from one form of practice to the other. This, as we interpreted it, was what was happening at AlphaIT. AlphaIT had the abstract ISS best practice that was translated to an organizational canonical practice – an ISS policy – and that policy was both constituted by and participated in the constitution of the situated practice of AlphaIT.

Implications for translation studies

In IS literature, translation has often been related to translation and transformation of knowledge across boundaries (e.g., Levina & Vaast, 2005; Levina & Vaast, 2006; Merminod & Rowe, 2012). Another stream of literature has, however, investigated translations in the context of management practice implementation (e.g., Powell *et al*, 2005; Morris & Lancaster, 2006; Nicolini, 2010; Nielsen *et al*, 2014). We contribute to the latter. We have here extended the concept of translation to the context of ISS policy implementation and to the discussions on how ISS policies and practices are internally born out of best practices (Hsu, 2009; Njenga & Brown, 2012). As ISS policy implementation often involves leaning on best practices, the analysis at AlphaIT suggests that translation provides an insightful concept to study and explain ISS best practice implementation and ISS policy implementation and contextualization.

While institutional theory has traditionally emphasized stability and similarity within organizational fields (DiMaggio & Powell, 1983) and previous studies in ISS management suggest that organizations should adopt identical practices (Hsu, 2009; Hsu *et al*, 2012), our study shows that best practices may not emerge unchanged while they travel from one context to another. In line with Nielsen *et al*'s (2014) argument about IT technologies, our study suggests that this change happens because best practices translate while they travel through existing organizational practices that modify and redefine them. At AlphaIT, through iterative and recursive translations, what resulted was a local appropriation of the best practices rather than a homogenization of organizational practices with best practices. This local appropriation was not merely about translation of words; it was also a matter of translating the foreign practices and the world they embody (cf. Backhouse *et al*, 2006) into local practices (cf. Leavitt, 2014). As such, our findings shed light on the little-known "processes through which actors translate broad ideas from very different industry contexts from their own into workplace practices" (Morris & Lancaster, 2006, pp. 207–208). Consequently, ISS practices across organizations may not emerge as identical simply by following the same set of ISS best practices. While, on an abstract level, it is possible to identify common characteristics of practices across organizations, closer analysis will likely show that the actual performance of these practices is never quite the same. The best practices become translated in relation to local needs and particularities (cf. Morris & Lancaster, 2006) that constrain the possible translations (cf. Hanks, 2014). Our findings thus challenge the often implicit idea that ISS practices should become identical across fields and organizations in order for them to be effective. In other words, at AlphaIT, the translated ISS practices were neither exact copies nor completely new, but sustained a resemblance to and a connection with the best practices in ways that fit their particular context and patterns of work. It would thus seem fruitful to think of best practices not as prescriptive recipes of ISS policy implementation but as ideas about the implementation.

More broadly, our study contributes to translation studies on the implementation of management practices that have emphasized how abstract field-level practices

Table 5 Implications for practice

1. When implementing ISS best practices, acknowledge that the best practices should be translated to fit the organization
2. When translating an ISS best practice into organizational practice, pay attention to and draw on existing local ways of working, and not only to non-local descriptions of work and best practices
3. In order to identify incongruent elements in the new ISS practices and existing organizational practices, expose new ISS practice (policy) in an early phase to employees' practice and collect feedback
4. Engage in employees' work in order to surface possible incongruence between ISS policy and organizational practice
5. Implement new practices in a way that is in line with other organizational practices (such as change management) and that acknowledges the differences between canonical and non-canonical practices
6. New ISS practice should be communicated and discussed with employees in a continuous manner rather than a one-off effort to increase employees' motivation and skills to enact the new practice
7. Notice that implementing an ISS best practice requires a translation not only from best practice to organizational policy but further to situated practice

are reified, refined, modified, and some practices are privileged over others when organizations transform these field-level practices into local practices. We support the previous arguments that actors at the recipient organizations play an active role in the adoption of management practices (Nielsen *et al*, 2014). As the actors engaged in the implementation, they came to see the ISS practices through the translations they helped to enact and mutually shape. We extend Morris and Lancaster (2006), who found that a hybrid of engineering, socializing, and teaching tactics were used to translate management practices to practice, by identifying factors that inhibited and positively contributed to the process of translation. We relate our findings to Nielsen *et al* (2014), who found that differing institutional logics inhibit translation, but extend this by suggesting more pragmatic causes – insufficient understanding of employees' work and the ISS managers' lack of engagement in organizational practices.

Implications for practice

In general, ethnographic studies may be well appreciated by managers, as such studies do not remove actors, actions, and events from the study descriptions (Ramiller & Pentland, 2009). In particular, this empirical analysis calls for increased managerial attention to different practices that shape ISS in organizations: canonical and non-canonical ISS and organizational practices. The study highlights seven implications for ISS managers (Table 5).

The first implication warns ISS managers of trying to implement ISS best practices without translating them. Translating means giving the best practice a meaning and boundaries in the context of an organization. Universal and general procedures of best practices are probably not directly applicable as such and trying to implement them without translation likely results in practices employees cannot and therefore will not enact in their work.

The second implication stresses the importance of acknowledging and accommodating the existing organizational practices in efforts to translate an ISS best practice into organizational practice. Organizational practice should be the starting point and source of information for the translation. Consequently, while ISS consultants and other externals can provide valuable advice, they cannot substitute local understanding and appreciation of local practices. A policy that is formulated largely or solely by external consultants may be incongruent with organizational practice. In other words, knowing how employees should work in theory cannot substitute for knowing (the contextual knowledge of) how they work in practice. The second implication further suggests that new ISS practices should not be too different from current practices or at least they should be compatible with organizational practice.

The third implication suggests that new ISS practices should be exposed to employees' practice early during the policy formulation process. Participatory approaches to policy formulation may be useful. They allow ISS managers to notice possible incongruences and requirements that employees cannot reasonably enact in their work. To illustrate one such requirement, Puhakainen (2006) describes an organization that strictly prohibited employees from taking any information out of organization's premises without written approval. However, in order to do their jobs, the employees customarily had to take their laptops and USB memory sticks to meetings held outside the organization. Such incongruence between ISS policy and employees' work practices could have been avoided if the policy had been exposed to employees' practice during the policy formulation. Then employees could have been instructed in secure means to take laptops and USB memory sticks out of the organization. Consequently, taking it for granted that ISS managers have the definitive authority, perhaps together with organization's top management, to formulate ISS policies may be a delusion; if those who have to enact the policy are not allowed to actively participate in policy-making and if organizational practices are not understood, turning policy into actions is hard at best. Along the same lines as the third implication, the fourth implication encourages ISS managers to engage in the work of their organization's employees. As this study

demonstrates, lack of engagement may result in a gulf between those who craft ISS policies and the like, and those who actually apply them in practice. This gulf may result in practitioners' misapprehension of the nature of the organizational members' work and practices and thus result in policies that organizational members cannot enact in practice. The gulf must be bridged in order to reach an acceptable policy that would translate into actions (Dhillon, 2007).

The fifth implication provides guidance on how to implement new ISS practices in a way that employees will be able to enact them in their work. Also, implementation should consider established organizational practices and manage ISS implementation in a way that is sensitive and congruent to those practices. For example, if an organization has a practice of allowing groups of employees to review new policies before approving them, this practice should be considered in the implementation. Further, the implementation methods should take into account that non-canonical practices and what can be described in an ISS policy are observably different. For example, in this study, from the ISS professionals' point of view, policy had to be sufficiently abstract for it to cover different situations. Not all situations employees will encounter in their work can be conceived in advance and thus are not documented in the policy. Therefore, the implementation should support employees' own initiative and skills, as no policy can describe all situations and, in the end, activity depends on employees' initiative and skills. The sixth implication provides further guidance on the same issue.

Finally, the seventh implication is at the heart of this study – implementing an ISS best practice requires translation from best practice to policy and further to situated practice. While having a policy may be enough to illustrate compliance to a certain ISS standard, it is the actual practices that help in securing an organization's information assets. If ISS managers focus solely on the canonical ISS practices, managers may overlook what it actually takes to manage ISS and prevent ISS breaches – the non-canonical practices of organizational members. The non-canonical practices – what happens in practice – likely foreshadow the success or failure of organizational ISS. Organizational ISS requires that best practices are localized and translated into organizational practice.

Conclusion

This study was motivated by the observation that, while ISS best practices are central to managing organizational ISS, their organizational application in practice has been largely absent from the literature. Therefore, this ethnographic study analyzed ISS policy implementation as a process of translation from an ISS best practice to an organizational ISS policy and further to situated practices in a single organization, at AlphaIT. The findings demonstrate the centrality of the organization's employees, their work, and organizational practices in the process. The challenges AlphaIT faced in its implementation efforts were not so much related to making an ISS policy from the prescriptions of the best practices, but implementing the ISS policy in a way that is sensitive to local ways of working and that is congruent with other organizational practices so that the ISS policy can become a part of existing practices and enactable by the employees. We argue that to implement ISS policy is to translate, and the success of the process is relational to *how* the translation takes place. AlphaIT provided an interesting and fruitful context in which to study the implementation process as it unfolded, but it only represents one example of the process. Future studies should focus on uncovering the process more broadly across different ISS best practices, contexts, and industries. Nevertheless, we believe the ideas on translation we have elaborated and developed here are likely to be present also in other settings beyond the single site of this study. Our study was not intended to make statistical generalizations, but – by relating the uncovered local ideographic details to broader theoretical ideas – generalizes to theory (Lee & Baskerville, 2003).

Although practice theory has already borne much fruit in IS research, new research avenues remain to be explored (Feldman & Orlikowski, 2011). We have explored these avenues by drawing on canonical and non-canonical practices and the concept of translation to arrive at a new understanding of ISS policy implementation. Organization studies have recently begun to explore the translation of field-level management ideas to situated practices. Moreover, we see fruitful future avenues emerging in the intersection of organization studies and IS research on ISS management that bring closer together the two disciplines (Orlikowski & Barley, 2001). The concept of translation may afford discussions between disciplinary boundaries and serve as a shared analytical tool to organize thoughts around how local practices emerge from ideas and practices that originate from a broader organizational or institutional context. Further, our analysis focused on the *how* aspect of the process of translation rather than on questions about *who* translates. As the concept of translation implies, in order to translate, translation competencies are central. We encourage future research to study how individuals' and collectives' competencies in performing translations engender variations in the resulting practices and what constitutes the optimal setup of those collectives (i.e., who should participate). Insufficient competencies likely increase an organization's risk of failing to translate the best practices to local practices and will lead to impoverished ISS policy implementation, which may result in the decoupling of the ISS policy from practice and expose an organization to unmanaged ISS risks.

About the Authors

Elina Niemimaa is a doctoral candidate at the Tampere University of Technology in the department of Information Management and Logistics. Her main research interests lie in the field of IS security where she focuses on information security management and on the practices of information security management.

Marko Niemimaa is a PhD candidate at the Turku Centre for Computer Sciences and University of Turku, Turku School of Economics in the department of Information Systems. His main research interests lie in the fields of IS security management, IS continuity and sociomateriality.

References

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

Almklov PG and Antonsen S (2014) Making work invisible: New public management and operational work in critical infrastructure sectors. *Public Administration* **92**(**2**), 477–492.

Arvidsson V, Holmström J and Lyytinen K (2014) Information systems use as strategy practice: A multi-dimensional view of strategic information system implementation and use. *The Journal of Strategic Information Systems* **23**(**1**), 45–61.

Backhouse J, Hsu CW and Silva L (2006) Circuits of power in creating de jure standards: Shaping an international information systems security standard. *Management Information Systems Quarterly* **30**(**Special Issue**), 413–438.

Barnes B (2001) Practice as collective action. In The Practice Turn in Contemporary Theory (Schatzki TR, Cetina KK and von Savigny E, Eds.), pp 25-36, Routledge, London, UK.

Baskerville R and Siponen M (2002) An information security meta-policy for emergent organizations. *Logistics Information Management* **15**(**5**/**6**), 337–346.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA and Boss RW (2009) If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal Information Systems* **18**(**2**), 151–164.

Brown JS and Duguid P (1991) Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation. *Organization Science* **2**(**1**), 40–57.

Brown JS and Duguid P (2001) Knowledge and organization: A social-practice perspective. *Organization Science* **12**(**2**), 198–213.

Bulgurcu B, Cavusoglu H and Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* **34**(**3**), 523–A7.

Callon M (2007) Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St. Brieuc bay. In: *Technoscience: The Politics of Interventions* (Asdal K, Brenna B, and Moser I, Eds), Oslo Academic Press, Oslo, NO.

Carlo JL, Lyytinen K and Boland Jr RJ (2012) Dialectics of collective minding: Contradictory appropriations of information technology in a high-risk project. *Management Information Systems Quarterly* **36**(**4**), 1081-A3.

Ciborra CU (1999) Notes on improvisation and time in organizations. *Accounting, Management and Information Technologies* **9**(**2**), 77–94.

Coles-Kemp L (2009) Information security management: An entangled research challenge. *Information Security Technical Report* **14**(**4**), 181–185.

Czarniawska B and Joerges B (1996) Travels of ideas. In Translating Organizational Change (Czarniawska B and Sevón G, Eds), pp. 13–48, Walter de Gruyter, Berlin, DE.

Czarniawska B (2004) On time, space, and action nets. *Organization* **11**(**6**), 773–791.

Czarniawska B (2009) Emerging institutions: pyramids or anthills?. *Organization Studies* **30**(**4**), 423–441

D'Arcy J, Hovav A and Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* **20**(**1**), 79–98.

Davison RM, Martinsons MG and Ou CXJ (2012) The roles of theory in canonical action research. *Management Information Systems Quarterly* **36**(**3**), 763–796.

Dhillon G (2007) Principles of Information Systems Security: Text and Cases. Wiley, Hoboken, NJ.

Dhillon G, Tejay G and Weiyin H (2007) Identifying governance dimensions to evaluate information systems security in organizations. In *Proceedings of the 40th Hawaii International Conference on System Sciences*, IEEE, Piscataway.

DiMaggio PJ and Powell WW (1983) The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review* **48**(**2**), 147–160.

Doherty N, Anastasakis L and Fulford H (2009) Information security policy unpacked: a critical study of the content of university policies. *International Journal of Information Management* **29**(**6**), 449–457.

Dougherty D (2004) Organizing practices in services: capturing practice-based knowledge for innovation. *Strategic Organization* **2**(**1**), 35–64.

Feldman MS and Orlikowski WJ (2011) Theorizing practice and practicing theory. *Organization Science* **22**(**5**), 240–1253.

Geertz C (1973) The Interpretation of Cultures: Selected Essays. Basic books, NY.

Gerber M and von Solms R (2008) Information security requirements – Interpreting the legal aspects. *Computers & Security* **27**(**5–6**), 124–135.

Gillon K, Branz L, Culnan M, Dhillon G, Hodgkinson R and MacWillson A (2011) Information security and privacy - Rethinking governance models. *Communications of the ACM* **28**, 561–570.

Hanks W (2014) The space of translation. *HAU: Journal of Ethnographic Theory* **4**(**2**), 17–39.

Hanseth O and Monteiro E (1997) Inscribing behaviour in information infrastructure standards. *Accounting, Management and Information Technologies* **7**(**4**), 183–211.

Hedström K, Kolkowska E, Karlsson F and Allen JP (2011) Value conflicts for information security management. *Journal of Strategic Information Systems* **20**(**4**), 373–384.

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

Höne K and Eloff JHP (2002) Information security policy - What do international information security standards say?. *Computers & Security* **21**(**5**), 402–409.

Hsu C, Lee JN and Straub DW (2012) Institutional influences on information systems security innovations. *Information Systems Research* **23**(**3-Part-2**), 918–939.

Hsu CW (2009) Frame misalignment: Interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems* **18**(**2**), 140–150.

Ingold T (2014) That's enough about ethnography!. *HAU: Journal of Ethnographic Theory* **4**(**1**), 383–395.

ISO/IEC (2013a) *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements*.

ISO/IEC (2013b) *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls*.

ISO/IEC (2014) *ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

Jarzabkowski PA, Le JK and Feldman MS (2012) Toward a theory of coordinating: Creating coordinating mechanisms in practice. *Organization Science* **23**(**4**), 907–927.

Johnston AC and Warkentin M (2010) Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly* **34**(**3**), 549-A4.

Johnston AC, Warkentin M and Siponen M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Management Information Systems Quarterly* **39**(**1**), 113–134.

Karjalainen M and Siponen M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, **12**(**8**), 518–555.

Karyda M, Kiountouzis, E and Kokolakis S (2005) Information systems security policies: a contextual perspective. *Computers & Security*, **24**(**3**), 246–260.

Klein HK and Myers MD (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. *Management Information Systems Quarterly* **23**(**1**), 67–93.

Knapp KJ, Morris RF, Marshall TE and Byrd TA (2009) Information security policy: An organizational-level process model. *Computers & Security* **28**(**7**), 493–508.

Kolkowska E and Dhillon G (2013) Organizational power and information security rule compliance. *Computers & Security*, **33**(**March**), 3–11.

Langley A (1999) Strategies for theorizing from process data. *The Academy of Management Review* **24**(**4**), 691–710.

Leavitt J (2014) Words and worlds: Ethnography and theories of translation. *HAU: Journal of Ethnographic Theory*, **4**(**2**), 193–220.

Lee AS and Baskerville R (2003) Generalizing generalizability in information systems research. *Information Systems Research*, **14**(**3**), 221–243.

Levina N and Vaast E (2005) The emergence of boundary spanning competence in practice: Implications for implementation and use of information systems. *Management Information Systems Quarterly* **29**(**2**), 335–363.

Levina N and Vaast E (2006) Turning a community into a market: A practice perspective on information Technology use in boundary spanning. *Journal of Management Information Systems* **22**(**4**), 13–37.

Merminod V and Rowe F (2012) How does PLM technology support knowledge transfer and translation in new product development? Transparency and boundary spanners in an international context. *Information and Organization* **22**(**4**), 295–322.

Miettinen R, Samra-Fredericks D and Yanow D (2009) Re-turn to practice: An introductory essay. *Organization Studies* **30**(**12**), 1309–1327.

Miles MB and Huberman AM (1994) Qualitative Data Analysis: An Expanded Sourcebook. SAGE Publications, Inc, Thousand Oaks, CA.

Morris T and Lancaster Z (2006) Translating management ideas. *Organization Studies* **27**(**2**), 207–233.

Myers M (1999) Investigating information systems with ethnographic research. *Communications of the AIS* **2**(**23**), 1–20.

Myers MD (2009) Qualitative Research in Business and Management. Sage, London, UK.

Myyry L, Siponen, M, Pahnila S, Vartiainen T and Vance A (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* **18**(**2**), 126–139.

Nicolini D (2010) Medical innovation as a process of translation: A case from the field of telemedicine. *British Journal of Management* **21**(**4**), 1011–1026.

Nielsen JA, Mathiassen, L and Newell, S (2014) Theorization and translation in information technology institutionalization: Evidence from Danish home care. *Management Information Systems Quarterly* **38**(**1**), 165–186.

Niemimaa M, Laaksonen E and Harnesk D (2013) Interpreting information security policy outcomes: A frames of reference perspective. In *Proceedings of the 46th Hawaii International Conference on System Sciences*, pp 4541–4550, IEEE, Piscataway.

Niemimaa M and Laaksonen AE (2015) Enacting information security policies in practice: Three modes of policy compliance. In Materiality, rules and regulation: New trends in management and organization studies (de Vaujany FX, Mitev N, Lanzara GF and Mukherjee A, Eds), pp 223–249, Palgrave Macmillan, Hampshire, UK.

Njenga K and Brown I (2012) Conceptualising improvisation in information systems security. *European journal of information systems* **21**, 592–607.

Orlikowski WJ (2000) Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science* **11**(**4**), 404–428.

Orlikowski WJ and Barley SR (2001) Technology and institutions: What can research on information technology and research on organizations learn from each other? *MIS quarterly* **25**(**2**), 145–165.

Orr JE (1996) Talking About Machines: An Ethnography of a Modern Job. ILR Press/Cornell University Press, Ithaca.

Orr JE (2006) Ten years of talking about machines. *Organization Studies* **27**(**12**), 1805–1820.

Powell WW, Gammal DL and Simard C (2005). Close encounters: The circulation and reception of managerial practices in the San Francisco Bay area nonprofit community. In Global Ideas: How Ideas, Objects and Practices Travel in the Global Economy (Czarniawska B and Sevón G Eds), Liber and Copenhagen Business School Press, Copenhagen, DK.

Puhakainen P (2006) A Design Theory for Information Security Awareness. University of Oulu, Oulu, Finland.

Puhakainen P and Siponen M (2010) Improving employees' compliance through information systems security training: an action research study. *Management Information Systems Quarterly* **34**(**4**), 767-A4.

PWC (2014) *Managing cyber risks in an interconnected world: Key findings from the global state of information security survey 2015.*

Ramiller NC and Pentland BT (2009) Management implications in information systems research: The untold story. *Journal of the Association for Information Systems* **10**(**6**), 474–494.

Ransbotham S and Mitra S (2009) Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research* **20**(**1**), 121–139.

Rees J, Bandyopadhyay S and Spafford EH (2003) PFIRES: A policy framework for information security. *Communications of the ACM* **46**(**7**), 101–106.

Rowe F (2012) Toward a richer diversity of genres in information systems research: new categorization and guidelines. *European Journal of Information Systems* **21**, 469–487.

Saint-Germain R (2005) Information security management best practice based on ISO/IEC 17799. *Information Management Journal* **39**(**4**), 60–66.

Schatzki TR (2001) Introduction. In The Practice Turn in Contemporary Theory (Schatzki TR, Cetina KK and von Savigny E, Eds), pp 11–23, Routledge, London, UK.

Schatzki TR, Cetina KK and von Savigny E (2001) The Practice Turn in Contemporary Theory. Routledge, London, UK.

Schatzki TR (2005) The sites of organizations. *Organization Studies* **26**(**3**), 465–484.

Schultze U and Orlikowski WJ (2004) A practice perspective on technology-mediated network relations: The use of internet-based self-serve technologies. *Information Systems Research* **15**(**1**), 87–106.

Siponen M (2005) An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems* **14**, 303–315.

Siponen M (2006) Information security standards focus on the existence of process, not its content. *Communications of the ACM* **49**(**8**), 97–100.

Siponen M and Iivari J (2006) Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems* **7**(**7**), 445–472.

Siponen MT and Oinas-Kukkonen H (2007) A review of information security issues and respective research contributions. *SIGMIS Database* **38**(**1**), 60–80.

Siponen M and Willison R (2009). Information security management standards: Problems and solutions. *Information & Management* **46**(**5**), 267–270.

Siponen M and Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *Management Information Systems Quarterly* **34**(**3**), 487-A12.

Siponen M, Willison R and Baskerville R (2008) Power and practice in information systems security research. In *Proceedings of the International Conference on Information Systems* (Boland R, Limayem M and

Pentland B, Eds), (14-17 December), Paris, Association for Information Systems.

Smets M, Morris T and Greenwood R (2012) From practice to field: A multilevel model of practice-driven institutional change. *Academy of Management Journal* **55**(**4**), 877–904.

Smith S, Winchester D, Bunker D and Jamieson R (2010) Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organization. *Managment Information Systems Quarterly* **34**(**3**), 463–486.

Stahl B, Doherty N and Shaw M (2012) Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal* **22**(**1**), 77–94.

Straub DW, Goodman S and Baskerville RL (2008) Framing the information security process in modern society. In Information security: policy, processes and practices (Straub DW, Goodman S and Baskerville RL, Eds), pp 5–12, M.E. Sharpe, Armonk, NY.

Suchman LA (2007) Human-machine reconfigurations: Plans and situated actions. Cambridge University Press, Lancaster University, Oxford.

Tsohou A, Karyda M, Kokolakis S and Kiountouzis E (2012) Analyzing trajectories of information security awareness. *Information Technology & People* **25**(**3**), pp. 327–352.

Tsohou A, Karyda M, Kokolakis S and Kiountouzis E (2015) Managing the introduction of information security awareness programmes in organisations. *European Journal Information Systems* **24**(**1**), 38–58.

Van Marrewijk A, Yanow D (2010) Introduction: The spatial turn in organization studies. In Organizational spaces: Rematerializing the workaday world (Van Marrewijk A and Yanow D, Eds), pp 1–16, Edward Elgar, Northampton, MA.

Von Solms R (1999) Information security management: why standards are important. *Information Management & Computer Security* **7**(**1**), 50–57.

Von Solms B and von Solms R (2004) The 10 deadly sins of information security management. *Computers & Security* **23**(**5**), 371–376.

Von Solms R and von Solms SH (2006) Information security governance: Due care. *Computers & Security* **25**(**7**), 494–497.

Warkentin M and Johnston AC (2008) IT governance and organizational design for security management. In Information security: Policy, processes and practices (Straub DW, Goodman SE and Baskerville R, Eds), pp 46–68, M.E. Sharpe, Armonk, NY.

Warkentin M and Willison R (2009) Behavior and policy issues in information systems security: the insider threat. *European Journal of Information Systems* **18**, 101–105.

Warkentin M, Johnston AC and Shropshire J (2011) The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems* **20**(**3**), 267–284.

Whitman ME (2008) Security policy: From design to maintenance. In Information security: Policy, processes and practices (Straub DW, Goodman S and Baskerville RL, Eds), pp 123–151, M.E. Sharpe, Armonk, NY.

Whittington R (2006) Completing the practice turn in strategy research. *Organization Studies* **27**(**5**), 613–634.