Organization Management Journal

Volume 9 | Issue 1 Article 9

4-1-2012

Leadership and the Psychology of Awareness: Three Theoretical Approaches to Information Security Management

Robert Holmberg
Lund University

Mikael Sundstrom
Lund University

Organization Management Journal, 9: 64–77, 2012

ISSN: 1541-6518 online
DOI: 10.1080/15416518.2012.666952

Routledge
Taylor & Francis Group

Leadership and the Psychology of Awareness: Three Theoretical Approaches to Information Security Management

Robert Holmberg[1] and Mikael Sundström[2]
[1]*Department of Psychology, Lund University, Lund, Sweden*
[2]*Department of Political Science, Lund University, Lund, Sweden*

The authors argue that information security management (ISM) would benefit from studies that examine the social and psychological mechanisms that, when in evidence, generate employee awareness of information security (IS)-related issues. Properly instilled, IS awareness has the power to engender a proactive wariness beyond mechanical guidelines, however detailed. To study how awareness travels in complex organizations, the authors devise a framework to catch mechanisms grounded in psychological and sociological theories. To illustrate the framework, the authors then turn to an empirical study of a medium-sized company where they sound out managers for definitions of IS and ISM; for initiatives intended to influence IS and IS awareness among employees; and for their views on learning related to IS and ISM. The study highlights the difficulties facing managers charged with IS matters, whose responsibilities are often considered peripheral by the general employee. The study also provides several pointers on how to go about the complex business of building awareness. *Organization Management Journal*, 9: 64–77, 2012. doi: 10.1080/15416518.2012.666952

Keywords information security management; information security; IS; ISM; awareness; leadership

THE SOFT SIDE OF INFORMATION SECURITY MANAGEMENT

In a worldwide survey among information security (IS) professionals, senior management support was identified as the highest ranking information security issue (Knapp et al., 2006). Attempts to identify the exact nature of such support/leadership are still rather thin on the ground, however. A wealth of studies emphasize the role of management support and leadership (e.g., Yukl, 2002, p. 2) pertaining to IS, but they tend to be cross-sectional and quantitative (Karyda et al., 2005) and rarely examine the actual mechanisms that explain the importance of management and leadership (there are exceptions, e.g., Siponen, 2000). As the literature on information and communications technology (ICT) and information security management (ISM) increasingly brings out, much of the early area research has focused on technical issues and solutions, to the relative detriment of the "human" side of ISM—that is, attitudes, beliefs, norms, behavioral patterns, leadership, culture, resistance etc. (e.g., Albrechtsen, 2007; Bock et al., 2005; Dhillon & Backhouse, 2001; Karyda et al., 2005; Rivard & Lapoint, 2010; Siponen, 2000; Siponen & Oinas-Kukkonen, 2007). It has also been suggested that one of the most important success factors when working with information security is employee awareness of the problem (e.g., Tsohou et al., 2008). The notion of awareness is one example how social and psychological processes have gradually entered the fields of IS and ISM. Sometimes this theme is complemented by one where the role of managers swings into focus—how their actions influence awareness and implementation of ISM (e.g., Karyda et al., 2005; Reddick, 2009). There are rather fewer examples of either theoretical or empirical contributions that deal with mechanisms pertaining to the *intersection* between those in formal management positions and other employees.

The purpose of this study is to identify and analyze mechanisms by which managers may help or hinder successful ISM in an organization. To this end, we design and apply an analytical framework consisting of three "tracks" that home in on different mechanisms that influence ISM activities. The framework is based on an understanding of IS and ISM that emphasizes the importance of learning in a social context and where qualities like information security awareness (ISA), "[which] aims at attracting the attention of all IS users to the security message, making them understand the importance of information security and their security obligations" (Tsohou et al., 2008, p. 210), active participation (rather than mechanical compliance; as conceptualized by Neal et al., 2000), and mindfulness rather than

This effort stems from the project "Legitimacy, Knowledge Creation and Practical Drift in Information Security Management," supported by the Swedish Civil Contingencies Agency by means of a multiyear grant. The agency does not influence any research decisions or project submission policies.

Address correspondence to Robert Holmberg, Department of Psychology, Lund University, Box 52, 22100 Lund, Sweden. E-mail: robert.holmberg@psychology.lu.se

mindlessness (Weick & Sutcliffe, 2001, p. 42) are perceived as critical for the long-term viability of IS.

Unlike other ISM studies (e.g., Karyda et al., 2005), we wish specifically to focus on the default ISM situation in an organization, that is, one devoid of recent or imminent ISM initiatives or drives, and where IS is but one of a number of managerial concerns. How IS fares in the day-to-day management business will, we argue, both have a pivotal impact on actual IS in the organization and, as we show, provide much-needed input when planning initiatives and drives to improve it.

With this in mind we finally put our nascent framework to the test and demonstrate how it can be used to anchor an interview study with a group of senior managers in a medium-sized utility company. The focus of the empirical study is how these managers may help and hinder awareness of information security issues in the normal run of things—that is, we repeat, when no major IS initiatives are in the offing.

MANAGING AWARENESS TO MANAGE INFORMATION SECURITY: THREE REASONS TO UNDERTAKE THIS STUDY

Reason 1: The General Importance of Awareness Processes

A guiding assumption in this effort is that the benefits of IS awareness, participation, and mindfulness—and thus of managerial policies that raise them—can be traced to the *flexibility* these qualities bring. A baseline level of judicious independence in the way employees relate to IS in the organization can prove an attractive complement to detailed lists of dos-and-don'ts. Awareness, participation, and mindfulness essentially improve the chances that individuals will act responsibly even in situations where there is little or no formal guidance. They additionally provide a living context for issued IS instructions. As Siponen (2000, p. 31) puts it, "Information security awareness is of crucial importance, as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness." Siponen focuses on the information security sector, but his remarks are just as valid elsewhere.

Reason 2: New Organizational Forms Accentuate the Need to Coach Employee Awareness

The various ways that management can bolster awareness and use it as a complementing vehicle for policy implementation are likely to become more important as organizations increasingly contain post-bureaucratic elements. Simply put, the network organization (e.g., Kenney & Florida, 1993; Ferlie et al., 1996; Powell, 1990) is an ideal inexorably on the rise. In the resulting, less tightly coupled organizational forms, associates become more nomadic, move in and out of projects, take on the guise of roving agents, belong to many different organizations at the same time, and so on. To maintain control at all in such a complex environment is a growing challenge facing managers, and strict information-mapping-plus-audit models are no panaceas, as studies of, for instance, accidents resulting from complex system breakdowns have shown (e.g., Rasmussen, 1997; Snook, 2000). Implanting or heightening psychosocial qualities such as awareness, participation, and mindfulness is one way to improve the chances that even semi-autonomous agents will act in ways that turn out to be beneficial to the wider organization.

Traditional models have typically promoted and/or made use of technology and formal administrative management tools, but increasing boundary-crossing, even nomadic, behavior patterns require a complementing approach to (information and other) security that is anchored in the *ways* individuals relate to each other.

Sociocognitive behavior theorists (e.g., Bandura, 1997) have confirmed that the individual's ability to motivate and regulate him- or herself becomes increasingly important in loosely coupled organizations. The psychology of leadership and management becomes a key consideration when we try to fashion methods to prepare and package information in ways that, ideally, maximize its perceived genuine relevance to targeted individuals and stimulate acceptable self-motivated IS behavior.

Reason 3: The Peripheral Status of IS Makes It Particularly Awkward to Manage

Unless the organization has security as its specific raison d'être, information security is, at best, a fringe interest to most managers and employees in it (e.g., McFadzean et al., 2007). Most employees would presumably agree, in principle, that defenses that keep the wheels moving by safeguarding information and/or help avert some nebulous disaster down the line are useful. At the same time, actual IS measures tend to intrude on work tasks that the individual employee considers primary. Employees may thus be tempted to circumvent them in order to carry out their primary work tasks more efficiently. This is a good illustration of the potential benefits of enhancing IS awareness. New and stricter guidelines will not necessarily weed out indifference or even hostility to IS measures. True awareness, by definition, will. Detailed dos-and-don'ts will not cover unforeseen exigencies. True awareness may.

The Challenge of Information Security Management

The chief information officer (CIO; we here use the title to indicate a manager responsible for IS matters) is thus faced with a particularly devious management task: to somehow overcome the intrinsic indifference or hostility to IS and induce users to embrace necessary measures as integral aspects of work.

Structure of the Rest of This Article

Figure 1 outlines the structure of the rest of the article.

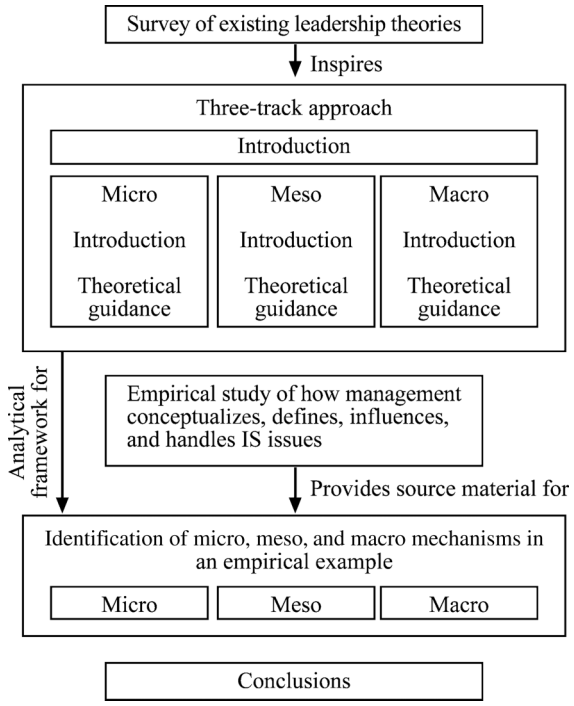

FIG. 1. The study at a glance.

THE PSYCHOLOGY OF LEADERSHIP AND INFORMATION SECURITY MANAGEMENT

While our focus remains intimately linked to leadership, we adopt a broader approach than is perhaps common in leadership studies. Yukl (2009) points out that the study of leaders' influence on learning processes in teams and organizations cannot be confined to mechanisms of person-to-person influence but has to identify and include other mechanisms as well. Heeding Yukl's suggestion, we thus prepare to outline a three-track analytical framework that is intended to catch theoretical input we feel may be fruitful, given our current focus. We emphasize that included theories are not exclusively focused on aspects of leadership, but have a considerably wider and more generic scope (covering, among other things, mechanisms relating to systems, representations of knowledge, learning processes, and individual cognition and behavior). In each case it will be possible to apply a leadership perspective, however. The idea, put bluntly, is to not be hemmed in by predefined notions of how leadership should be studied, but to remain open to a range of candidates. This is also the reason why we have decided to develop a multitrack framework (rather than a more open-ended counterpart): We feel that its very structure will force us to consider a wider range of potential mechanisms and supporting theories when studying how leadership matters in relation to the management of IS. The tracks should thus not be viewed as strictly discrete; they are complementary pointers, and overlaps should be expected.

We have suggested elsewhere (Sundström & Holmberg, 2008) that awareness-making and employee ability/willingness to integrate IS aspects and policies in everyday work activities can really be understood as interlinked aspects of a recurring social learning cycle (we build on Boisot, 1998). While such a perspective for the most part calls for a bird's-eye (macro) view on the "architecture" of grand-scale organizational learning processes, it remains firmly rooted in micro-level sociocognitive theories on interaction and behavior. Between these extremes we find a meso level where learning processes within individual organizations are the major concern. Improved grasp of the learning processes that belong to any of the three levels will improve management ability to gauge, and possibly manage, how organizational members perceive, think, and behave vis-à-vis IS. We suggest that the ancillary status of IS policies in most organizations and the changing nature of organizations themselves make it particularly important to consider all three levels simultaneously. The framework thus comprises the following three tracks: a micro track (focusing on cognition and behavior); a meso track (representations of knowledge in social systems); and a macro track (systems design; Table 1). To each track we affix a number of theories, and furnish brief explanations or elucidations when we feel that the context does not provide enough intuitive pointers.

APPROACHING LEADERSHIP AND INFORMATION SECURITY MANAGEMENT: THREE THEORETICAL TRACKS

Changes in the organization of work have brought to the fore the growing importance of the ability to reflect about one's actions and learning as evidenced by the burgeoning literature on (generic) learning, organizational learning, and knowledge (Argyris & Schön, 1996; Boisot, 1998; Boisot & Li, 2007; Lipshitz, Popper, & Friedman, 2002; March, 1991; Nonaka, 1991). The increasing complexity of production processes and rapid technological development have prompted the development of theoretical models that aim to improve our general understanding of complex system-level dynamics (e.g., Perrow, 1984; Rasmussen, 1997). There are also examples of more narrowly focused models dealing with failures (and how to understand failures) in complex systems, for example, the theory of practical drift, where Snook (2001) notes that the unconscious evolving of practice may well improve on formal protocol in most cases (which is why it occurs at all), but also disregards specific but highly unusual exigencies. Snook also notes that when protocol aberrations were observed, solutions tended to revolve around a hardening of protocol where more detailed rules were issued to weed out the problems. As the dynamics that led to the continual reinterpretation of protocol were left untouched, this approach was unable to "enforce" the sought-after compliance, however. New instructions were in effect fed into the same machinery that had processed the old instructions, and results were similar. We find Snook's studied case particularly relevant because information security management is to ward against exigencies so rare that they will hardly rouse or even rattle the average employee in a typical organization. Practical drift helps explain the natural process

TABLE 1
Three tracks at a glance

Level/track	Focus, mechanisms, mediums	Actions/behaviors related to leadership	Relevant psychological and sociological theories
Micro: cognitive, behavioral	Individual's goals, self-regulation, skills, feedback, direct interaction	Communicating standards, norms, goals, and values; providing feedback; acting as a model to enhance self-efficacy; coaching leadership qualities; etc.	Bandura (1997) Ajzen (2005) Latham and Locke (1991) Ilgen and Davis (2002) Kluger and DeNisi (1996) Hannah and Lester (2009)
Meso: learning and knowledge	Representations of knowledge; social systems (i.e., groups, teams, communities of practice, departments); social structures	Facilitating learning; knowledge creation; knowledge sharing; acting as a model in dealing with defensive routines; intellectual stimulation; base decisions on valid data; using boundary objects. Measurement systems, performance indicators, evaluations, etc.	Argyris and Schön (1996) Nonaka (1991) Boisot (1998) Lave and Wenger (1991) Lipshitz, Popper, and Friedman (2002)
Macro: systems design	System-wide design and strategy; reflections about institutions; understanding representations of feedback mechanisms; organization-wide strategy	Representing, reflecting on, evaluating and (re)designing systemic features; shaping feedback processes and impulses in the wider system; carefully designing boundary objects (strategies, policies, plans rules, performance indicators); etc.	Rasmussen (1997) Snook (2000)

of "wariness atrophy" in these situations—and we argue that awareness needs to be taken into account if IS managers truly wish to offset these naturally occurring and debilitating forces.

These studies all underscore an important fact: Work in large contemporary organizations is typically so knowledge-intensive that it must be mediated and managed by means of various abstract representations such as plans, project management tools, accounting systems, performance indicators, and so on. In such an environment, skilled leadership has a lot to do with the ability smoothly to negotiate and manipulate these knowledge maps (which are in effect simplified real-world proxies). Since these abstractions in turn have concrete bearing on the interaction between organizational entities, on organizational and social processes, and on the perceived context of individual employees, they can help us identify mechanisms through which leadership action truly impacts IS. Bluntly put, certain forms of manipulation of these abstractions will indeed organize and package information in ways that make it travel well, and trigger the "self-motivated IS behavior" we discussed earlier, while other forms of manipulation of the abstractions will in effect constitute (IS) management duds.

The Micro Level: Influencing People Through Interaction—A Cognitive Behavioral Track

A critical aspect of leadership involves "direct" influence (e.g., Yukl, 2002). Tactics such as rational persuasion, consultation, personal appeals, and pressure may be used to achieve this end. In a study of how CIOs influenced management peers, Enns et al. (2003) found that rational persuasion and personal appeals were correlated with commitment from other managers, whereas pressure and exchange were correlated with resistance. It would seem pertinent to take a more detailed look at the mechanisms that manage to engender commitment, so we turn to theories of social psychology and social cognition.

One way of studying how leaders influence subordinates and peers is to analyze their impact on attitudes, perceptions of norms, and behavioral intentions (Ajzen, 2005), and how influence attempts affect individuals' goals, self-efficacy, and other self-regulatory processes (Bandura, 1997). Hannah and Lester (2009) suggest that in order to encourage organizational learning, managers have to lead the way on a micro level, using direct interaction with their coworkers to nurture nascent "developmental readiness" (p. 37). It becomes a matter of promoting a general openness to learning, and helping coworkers realize their capacity for critical thinking. An improved ability to monitor and evaluate their own thinking processes will, in short, prepare them for further development and enable them to act as "knowledge catalysts" in Hannah and Lester's (2009) terminology. Latham and Locke (1991) underscore the importance of goal-setting for individual performance and argue that goals help the individual to direct his or her attention on to specific aspects of the environment, making him or her better able to extract relevant information to evaluate performance. Goals also have a critical impact on self-regulation in that they help to

focus efforts, and thus boost intensity and strengthen tenacity (Hannah & Lester, 2009).

External feedback does not in and of itself necessarily lead to changes in behavior or improved performance (Kluger & DeNisi, 1996). This is an important point, and one often overlooked in audit-based organizational cultures. Instead, improved performance depends on how the individual evaluates the outcome of his or her actions; on to what extent he or she is dissatisfied with that outcome; and on whether he or she has a high level of self-efficacy and set goals for improvement. Feedback can indeed support such processes, but can also inhibit them. The crucial role of self-efficacy beliefs ("people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances"; Bandura, 1997, p. 391) has been highlighted in a range of studies. Ilgen and Davies (2002) analyze how people deal with negative feedback, and discuss how leaders may help coach the individual's goal attainment strategies and self-regulation processes.

The communication of goals, standards, and norms thus has an important role in shaping the individual's efforts. Thoughtful feedback, active involvement in self-regulation, strategy development, and the strengthening of self-efficacy beliefs are examples of how leaders can guide organizational members on a micro level—mostly relying on direct interaction. Benefits will be evident when a leader helps to direct coworkers toward clear, challenging (yet realistic), and measurable goals and in the process acts as a role model and facilitator to fortify coworkers' self-efficacy (Bandura, 1997; Latham & Locke, 1991). Ajzen's (2005) theory of planned behavior offers another way to understand the mechanisms involved when leaders influence organizational members on the micro level. According to Ajzen, behavioral intentions are determined by (a) attitudinal beliefs (e.g., a belief that regularly changing passwords will indeed raise the level of information security and that this is in fact important for operations etc.), (b) normative influence (the degree to which significant others are perceived to want me to change password regularly), and finally (c) behavioral control (do I think that I have control over the behaviors needed to be able to change passwords?). Behavioral control is of course closely related to competence and self-efficacy beliefs. According to this theory, leaders who want to influence their coworkers' behavior should pay attention to their attitudes, norms, and perceptions of behavioral control, and consequently adapt their own behavior in ways that will have the most impact.

The Meso Level: Influencing People Through Boundary Objects—A Learning and Knowledge-Centric Track

The meso level includes and relates to representations of knowledge, and how these are related to effective action and learning processes—usually within a social context.

A crucial element in any discussion about knowledge is the realization that there are several different types of knowledge—for example, the distinction between declarative knowledge (knowing that X is so) and procedural knowledge (knowing how something is accomplished). Based on philosophical works on knowledge (e.g., Polanyi, 1958), management scholars have drawn attention to the importance of tacit knowledge, arguing that "creation of knowledge" in organizations can in reality be viewed as transformation processes between tacit and explicit knowledge and vice versa (Nonaka, 1991). Argyris and Schön (1996) make a distinction between the explicit reasons we give for our actions and the more implicit models that can be induced from our actions. Boisot (1998) goes further and suggests that knowledge can be fruitfully conceptualized as varying in codification, abstraction, and diffusion, resulting in different knowledge regimes ranging from embodied (mostly tacit) knowledge via narrative knowledge to abstract symbolic (mostly explicit) knowledge. Lave and Wenger (1991) highlight how knowledge can be regarded as situated and thus understood as an aspect of a practice embedded in everyday work. Another theme in the meso-level literature concerns representations of knowledge in the form of mental representations, theories, rules, maps, databases, stories, routines, and so on.

Social and cultural contexts also have important repercussions on knowledge and learning processes. Boisot (1998) discusses how (archetypal) bureaucracies, fiefs, clans, and markets impact knowledge and knowledge creation in specific and distinct ways, while practice-oriented researchers like Lave and Wenger (1991) focus on concepts like communities of practice—contextual binders that cut across organizational charts to focus on actual interaction patterns.

A specific and intriguing angle on social and cultural aspects and how they influence learning processes has been presented by Argyris and Schöns (1996) in their study of defensive reasoning and routines appearing within organizations. Lipshitz et al. (2002) have developed a model where organizational learning mechanisms (practices such as debriefing after action) in conjunction with organizational values that support learning are identified as fundamental for productive learning.

However conceptualized, these efforts—unlike those residing on the micro level—all attempt to frame the processual, even cyclical, nature of learning in and by organizations. It is relatively easy to connect these conceptualizations to the focus on abstractions we have discussed already; it then becomes a matter of somehow wedging in the abstracted knowledge repositories in the information models.

The Macro Level: Influencing People Through System Design—A System Architecture Track

The systems framework may be seen as even more far-reaching in that it concerns representations of the many levels (of the totality of a system) that surrounds a task or a role and the focus is on the systemic mechanisms generating behavior.

Rasmussen (1997) provides a macro perspective when he draws attention to system mechanisms that generate certain types of behavior. While his focus is trained on the analysis

of accidents, the suggested perspective may also be applied to organizations and organizational roles in general. Rasmussen suggests that the actor—the occupant of a specific role—is situated in a "space of possibilities" within which the actor retains a certain liberty of action. Specific mechanisms in the systems (typically external pressure to increase efficiency or an internally derived drive to minimize personal effort) tend to push the role-occupant toward the *boundaries* of that space—and sometimes stretch them in ways that can lead to accidents or other undesired results. Rasmussen describes this process as a structural migration toward boundaries and argues that attempts to enforce stricter controls or to fight deviation head-on are not viable long-term solutions. Rather, efforts should be made to make "the boundaries explicit and known and [to provide] opportunities to develop coping skills at boundaries" (p. 191). Snook's (2000) concept of practical drift shares many attributes with the Rasmussen framework in that it identifies normal organizational processes where action-based logics and rule-based logics clash and can lead to fatal accidents, even while individuals all act in good faith (Lundestad & Hommels, 2006; Snook, 2000). For us, Snook's conceptualization holds extra allure as he explicitly identifies the interface between tightly and loosely coupled systems as the source of many problems. If, as we have argued, nomadic work practices become gradually more prevalent, the number of such interfaces will inevitably multiply, which will in turn aggravate structural problems.

ACROSS THE TRACKS: INSIGHTS

As we have indicated, the three tracks are not discrete—and were never meant to be. If anything, existing overlaps are illuminating. For one thing, theories across the spectrum tend to emphasize the role of the individual in organizations. There appears to be general agreement that it is unwise to consider the individual as a passive rule-follower or conduit of someone else's will. "Rules," like set tasks, can be, and will be, subject to constant review by the individual, and will be adjusted when interaction with the physical and social environment so demands. This is bad news for prevalent audit-and-certify control models, as there cannot, by definition, be a "perfect" way of doing things no matter how ardently you try to model ideal information flows. An individual's behavior in an organization can be perceived as a holding pattern on which a number of forces—micro, meso, and macro—are constantly at work. Here we get the theoretical framing of the increased problem of managing loosely coupled organizations including nomadic elements: More but weaker forces affect organizational holding patterns, which in turn expands individuals' "space of possibilities," and with it the contextually determined freedom to interpret management demands.

We similarly get a theoretically grounded understanding of the particular challenges facing information security managers. Managerial governance of aspects central to what the organization "is about" tends to be heeded more than managerial governance of (perceived) nonessential aspects (such as information security) because many different kinds of forces push roughly in the same direction. When managers feed such "essential" information into the abstract representations we have already discussed (plans, project management tools, accounting systems, performance indicators, etc.), they essentially feed expectations into a system that is—on all levels—already primed to relate to them.

The tracks also furnish some ideas how to overcome these obstacles. Managers may, for instance, gather data on how different pressures in the wider system actually affect the workers' psychosocial context. Dialogue and reflection with such a focus—which is typically beyond the managerial beaten track—will create a more robust understanding of the factors that, left unchecked, risk engendering undesired practical drift and migration toward boundaries. Sharing such understanding in an organization may be a step toward greater awareness, and awareness is a first step on the winding road to active interest, and, ideally, the perceptional shift of "nonessential" aspects (e.g., ISM) to the point where they are truly regarded as natural aspects of the organizational raison d'être (whereupon the self-regulating forces will come into play).

The development of shared understanding/mental models among employees, and especially within groups of managers charged with managing and leading ISM in the organization, is a critical component in developing awareness. Examples of mechanisms that can contribute to this include the support of connectivity and communality through interorganizational communication and information systems as described by Monge et al. (1998). Their approach shows how a shared information infrastructure (such as, say, a busily used intranet or shared database) is not "just" a beneficial information exchange mechanism and connectivity medium. It also has a communal impact, as it creates a common frame of understanding of related problems. This can make it easier to approach common challenges, including IS ones, as well as improve learning opportunities across the organization. By extension, then, the design and implementation of such connectivity platforms carry with them a usually overlooked information-handling element that a knowledgeable management can turn into a strategic information management asset.

To further aid this transformation, the next step would be to consider different design options based on the evolving understanding of the meso (learning/knowledge) track. Facilitating learning processes by means of mechanisms like audits, evaluations, and debriefings, where managers themselves (acting as role models) are subjected to frank and open enquiry and criticism will encourage employees openly to discuss wider implications of policy changes (Argyris & Schön, 1996; Lipshitz, Popper & Friedman, 2002). Misfortunes and acknowledgment of managerial fallibility carry with them a great and often untapped learning potential in the wider organization. Micro-level insights finally provide hints how managers may communicate clear goals and standards, provide feedback, and in some cases coach employees in the way to manage themselves in relation to, in this case, information security.

FROM THEORY TO EMPIRICAL STUDY AND BACK

The Empirical Case Study—An Introduction

We have studied a medium-sized utility company in northern Europe with around 500 employees dispersed across a relatively wide geographic area and a number of different sites. The enterprise is organized as a concern with a number of subsidiary companies.

We conducted interviews with eight managerial-level informants in the company: the CEO, the sales manager, the information technology (IT) manager (formally in charge of IS matters), the human resources (HR) manager, the information manager, two executives from subsidiary companies, and the company's security coordinator. All interviewees are well educated, are experienced managers in the company (having had a number of roles in the case company and its subsidiaries), and have been involved in a major effort to reorganize the business. We refrain from providing still more complete demographic data as the information provided in the article combined with such demographic data could conceivably be used to reveal the identity of the company—and thus the informants themselves—thus compromising promised anonymity.

The interviews were part of a pilot study set up to probe how a group of managers perceived IS and ISM issues in the company. The idea was to improve understanding of the "default" IS/ISM situation, that is, a situation not characterized by any major IS initiatives or drives. This would in turn help us see certain needs that potential future initiatives could and perhaps should be designed to address.

The methodological approach was guided by scientific realism (Pawson, 2007) in that we regard the responses from our informants as—in principle—reflecting their behavior and attitudes, as well as the relevant organizational and social circumstances. The rationale for working with this relatively small number of informants from one company is that the case provides us with access to a number of key decision makers where the intersection between leaders' actions and understandings, on the one hand, and the actual development of ways of working with IS, on the other, was sharply highlighted. In this effort, we use the case to demonstrate our theoretical tracks and probe their proposition. The methodological approach could thus not be described as either exclusively deductive or inductive, but as a form of abduction (e.g., Alvesson & Sköldberg, 2009). Important to note is that the sample does not allow for statistical generalization claims.

The (semistructured) interviews each lasted between 1 and 1.5 hours, and were organized around four central themes (the b1–b2 designation reflects the fact that these two closely related themes are analyzed under the same heading where we present the findings):

a. Definitions and general understanding of IS and ISM by the interviewees (the aim was to trawl for uncoached and as far as possible decontextualized notions of what IS might entail).

b1. Examples (if any) of initiatives taken to raise awareness among employees (the question was designed to narrow the discussion from abstract ideas or ideals (as answered in (a)) to on-the-ground measures in the company that they are aware of, which they somehow consider IS-relevant.

b2. Experiences of positive and negative outcomes of various measures (here the ISM process becomes the main focus).

c. Examples of learning related (in a wide sense) to IS and ISM (we here probe for experiences of ISM-related processes: what worked, what did not work).

Interviews were recorded and notes were taken during the interviews.

The purpose of the interviews was to explore managers' conception of ISM and how they worked with IS issues in the context of this organization, with its structure and history. Based on the studied literature and on preliminary interviews with a manager responsible for security issues, and a senior advisor on information management, we designed an interview guide. The questions were open-ended to induce the managers to voice their views and experiences in their own words. We particularly wanted to avoid asking questions that might suggest that they *ought* to have done a number of things—creating an audit-like situation or a feeling that they were being interrogated. The questions were meant to have a positive tone that encouraged managers to share their views and experiences as freely as possible. Each interview began with questions about the interviewee's general background and history in the company. It then homed in on the four themes with open-ended questions such as: "What comes to your mind when you hear the concept 'information security'?" "Can you give any examples of specific measures that the company has undertaken to improve ISM?" "What effects, good or bad, did those measures create?" "We have heard about measure X. How would you change X next time, and why?"

The recordings were transcribed and merged with the notes to provide an overview of what was said in relation to the four themes. Each interview was analyzed in relation to the themes, and the general "answer patterns" are reported in the following section. A summary of the study (including an overview of the findings) was presented and discussed in a seminar in which four of the interviewees participated. Where required, details and interpretations of data have been further corroborated by means of follow-up correspondence with relevant interviewees.

DEFINITIONS OF IS AND ISM/MEANINGS OF ISM: EMPIRICAL FINDINGS

No Shared or Formal Definition of IS

The interviewees did not provide a coherent and shared definition of either information security or information security management. The chief executive officer (CEO) knowledgeably discussed a wide variety of security-related issues, and expanded on how the company as well as the sector at large had historically worked with these issues and how they worked with them now. Five of the remaining interviewees mentioned

business-related information as something that had to be protected to some extent. All interviewees referred to the company's "IT handbook" as a general source of information. It did not appear to be an obviously "living" document, however, as no interviewees provided pertinent details from it or presented how they had used it.

IS Issues "Owned" by the IT Manager

The interviewees consistently referred to the company's IT manager as someone who knew about these things and who did a very good job. The sales manager described how this worked in the organization: "The IT manager has built a system that works for our needs; he is out and about [talking to people]. . . . He has a strategy and a way of thinking that help him explain that we cannot have [certain software solutions] now but later; we are well ahead [with a] system for authorization; [we] have dealt with the virus risk; [he is] working proactively; I have great confidence [in him]. . . . Previously you brought along your laptop—now he has changed that so you access [systems] through the laptop, you don't have things in the laptop."

As exemplified by the quotation, the interviewees were very confident that the IT manager had a firm grasp of these issues and that he had implemented proper technical procedures, strategies and policies. This confidence was to a large extent vindicated in the interview with the IT manager who clearly had the most sophisticated views on IS and ISM among those interviewed.

A Manager as an Island? Parochial Outlooks on IS and ISM

While the CEO discussed almost all possible combinations of security risks, the other informants tended to focus on issues that were closely related to their own area of expertise and responsibility. The senior manager responsible for sales discussed the possible risks of leaks from databases containing customer information. He also perceived this as being related to a more general tension between security and openness, where efficient work processes have to build on openness and trust, but where you restrict access to certain kinds of information to a smaller group of employees—particularly during critical negotiations with customers. Managers who were more directly responsible for production tended to view security in terms of reliability of production processes, and safety issues related to the potential physical dangers involved in production processes. The information manager focused on how the company dealt with information and public relations (PR) issues, especially as they related to who was authorized to speak on behalf of the organization about various issues. For the security coordinator, the focus was associated with the challenges intrinsic to working with a wide array of security issues—and spreading awareness about them.

Comments

The responsibility for—and knowledge of—IS and ISM has been informally delegated to the IT manager. While the interviewees seemed content with this division of labor, there was some evident embarrassment over what they perceived as their difficulties in presenting a formal or more coherent definition of information security and how they worked with information security management in the company. Some of the interviewees also expressed concerns about their being too naive in relation to security issues. To some extent this notion would seem to be corroborated by the fact that there were very few spontaneously offered examples of risks related to terrorism, sabotage, and so on.

In the interviews, security was typically discussed in terms of broad themes such as ethics and trust, and responses seldom focused on technology or IS per se. The interviewees demonstrated thorough understanding of their respective responsibilities, but these responsibilities evidently anchored their responses to questions about IS by connecting it to something more familiar. The managers' views on IS/ISM can roughly be divided as follows. In part IS/ISM was gladly delegated to the competent IT manager. In part it was considered a somewhat nebulous phenomenon that they approached through concepts and understandings based on their own primary responsibilities—and thus in ways that radically differed from others' perceptions of it. As a managerial concern, IS/ISM was slender, where descriptions—and possibly understanding—reflected facets of one's own work practices (rather than stemming from "big picture" analyses), and where narratives tended to stray to examples of irregular behaviors or system malfunctions as perceived or experienced from this local perspective.

INFORMATION SECURITY INITIATIVES AND THEIR CONSEQUENCES: EMPIRICAL FINDINGS

IT Unit: From Maintenance/Support to Developer of Strategy

Since the turn of the century, the company has effected a number of changes that have had wide-ranging repercussions for both business and general security. As a consequence, the way that the company uses ICT has changed considerably, and the IT section has evolved from a "technical" department focused on running and maintaining IT hardware, to one that is guided by a clear strategy and that "owns" the systems and related security issues.

Major changes included the separation of supervisory control and data acquisition (SCADA) functions from administrative systems (where they had previously been integrated); the implementation of a unified login service; the establishing of procedures to integrate IT systems in subsidiary companies and new acquisitions; national authority-compliant system documentation; a written policy for computer use and Internet access; and the removal of all end-user computer administrator privileges.

Certain measures are mostly oriented toward physical security (e.g., locked doors between floors in office-buildings, and the relocation of servers to secure areas.

Difficulties Related to Lack of Knowledge and Attitudes

The IT manager described how users make a substantial investment of resources when they familiarize themselves with existing systems, and how these sunk costs tend to make them focus on specific "vital" (from their point of view) subprocedures when asked to evaluate potential replacements. He emphasized that it is generally difficult for normal users to free themselves from their own daily concerns to appreciate wider structural implications—including how security may be affected.

When users were stripped of their local computer administrator privileges, it led to a number of discussions with employees who were upset that their freedom to install software as they saw fit had been curtailed. Another issue mentioned in the interviews was that too many passwords can be a nuisance and constitute an unwanted and continual obstruction when going about daily work life.

Management by Walking Around

In the interview with the IT manager (and further corroborated in the other interviews), it became clear that the IT manager's preferred mode of operation (MO) is continual, on-the-floor interaction with management teams, heads of departments, and local IT reps. This includes regular meetings where policies, strategies, and explanations (i.e., the practical understanding of policies and strategies) are discussed. The IT manager emphasized that—in addition to putting formal documents on the intranet—it is essential to understand the way in which work with (policy) integration is actually dealt with on the floor, if IT (and ISM) strategy is to be more than a dead letter.

> And that's the reason I walk around talking [to people]: there is no point writing books, or instructions or putting it on the intranet. You have to do it like this, talk, stand up for your viewpoint and explain. What we are also doing is . . . you sign . . . in order to [get internet access], you have to sign . . . that I have read the IT manual, that I have read it and that I will from now on keep my self up to date with things. (IT manager)

Comments

The broad ICT measures adopted by the company have impacted a variety of core business practices. In part, changes have been brought about as a consequence of a proactive strategy (sandboxing of SCADA systems, integration, server solutions, fire walls, and so on). In other cases, measures have been reactive: the result of incidents, such as computer thefts, inappropriate use of the Internet, and so on.

From individual employees' points of view, some of these measures can be experienced as unwanted restrictions of their autonomy. Stricter policies about acceptable software, administrator privileges, use of printers, and so on can in some cases be difficult to understand and to accept. They can also be perceived as illegitimate restrictions, not only of personal autonomy but also of one's professional discretion. This is where the IT manager's emphasis on continual interaction and dialogue seems particularly prudent. In instances where employees find it difficult to reconcile particular demands with their primary task and/or the prevailing work ethos, written policies are unlikely to suffice. A complementing strategy of interaction and dialogue will be more successful when knowledge, norms, and attitudes are to be altered.

EXAMPLES OF LEARNING RELATED TO IS AND ISM: EMPIRICAL FINDINGS

Learning From Incidents

Reactions to different kinds of incidents and problems that have occurred over the years, and the measures that have been implemented as a consequence, constitute a distinct and interesting learning process. The interviewees gave little indication that the company had a coherent, formalized ISM policy, preferring to offer different examples of incidents and subsequent measures when asked about information security.

An important event that all interviewees discussed was a natural disaster some years back that had had a profound impact on the company and its customers. The event stretched contingency plans beyond their limits, and exposed a number of organizational weaknesses. The realization that the company had been ill prepared for problems on that scale led to a comprehensive review of existing crisis management structures. The company has since improved its ability to maintain operations and keep customers and media up to speed even in highly abnormal operating conditions.

The shared experience also had an impact on internal social systems, however. The way employees had to marshal all resources to overcome the difficulties improved the general esprit de corps, and successful managers were provided with a "halo" of recognition.

Comments

The event itself seems to have become a crucial part of the company's shared mythos, and a virtual litmus test when crises and crisis management is discussed ("how would proposed measure X have worked in the experienced disaster," etc.). The informants tended to relate questions about "information security" to "risk," and then to their experience during the event—and what they had learned from it. Indeed, the event was so pervasive a theme in the interviews that it seems warranted to describe it as a formative experience with the continuing power to form perceptions, thinking, and identities.

TRACKING BACK: CONNECTING EMPIRICAL FINDINGS TO THEORY

Macro Track—A Systems Outlook

For managers to be able to relate in a skilful way to the wider systemic processes—and their relationship with the "space of possibilities" surrounding individual employees—they have to have access to mental representations of these systems, and be able to share perspectives that can support a process of critical inquiry. This is especially applicable when systemic processes like practical drift (Snook, 2000) and migration toward boundaries (Rasmussen, 1997) are in operation. In order to deal with phenomena of this kind, external mechanisms of social, economical, and technical nature have to be considered over time. The last decade has seen the company go through a process of transformation that has deeply affected its operations. ICTs have become key aspects of the company's production, distribution, marketing, customer relations, and sales support systems. This development has been relatively rapid, and ICT integration has become gradually more sophisticated, as exemplified by the IT manager's work with the IT strategy. At the same time, interviewee responses to questions about information security management clearly indicate that the ICT strategy in general, and ISM issues in particular, remain a separate domain. Discourses on security generally revolve around production systems and related safety and security issues. The interviewees demonstrate a close familiarity with these production technologies and with how the state's role in infrastructure maintenance—and thus general security awareness in this field—has changed over the last 20 years. There are fewer signs that a shared perspective on the strategic role of ICT and IS has manifested itself, however. ICTs may have become pervasive throughout the organization, but "problem ownership" and strategic identification of latent threats have de facto remained exclusive IT manager concerns.

One tenable theoretical interpretation is that the company is in fact still in the middle of a transformation process where ICTs gradually evolve to become pivotal aspects of all production and business processes. McFadzean's (2007) contention is that such transformation will eventually lead to the upgrading of ICT issues to the strategic planning level, which will in turn engender more active consideration of IS issues.

A basic question in a study such as this one is how you accelerate this process of maturation. While a high level of technical IT security has been attained—in no small part a testament to the IT manager's competence—the ability of management as a whole to engage in critical reflection and debate on how its members work with IS from a systems perspective (e.g., in the sense of Rasmussen's notion of migration toward boundaries and Snook's practical drift) seems to be relatively stunted. The lack of system representations, suitable metrics, and shared mental models makes these kinds of deliberation still harder. A critical consequence of such a state of affairs is that a limited and/or deficient discourse on systemic processes on the managerial level severely limits/undermines individual managers' ability to work with learning processes and lead/influence their coworkers truly to integrate these issues in their work practices. There is consequently a risk that we get fiefs of IS understanding that may hinder the IT manager's attempts to implement company-wide policies. In a rather more nomadic organizational context—a future scenario worth serious consideration—such fiefs can become very small indeed.

We argue that in order for managers to be able to support information security awareness and be better equipped to deal both with risks and various interventions/security measures they have to have shared understandings/mental models of how ICTs work in the organization. This can in fact be regarded as a basic requirement for ISM that is aligned with the organization's structure, task, and strategy and that can be managed both with flexibility and over the long term.

Meso Track—A Learning Process Outlook

The informants gave no examples of specific organizational learning mechanisms in the form of evaluations, after-action debriefings, and so on (as discussed by, e.g., Lipshitz et al. [2002]). With the exception of the IT manager, nor did they refer to any systematic gathering of IS and ISM data. Although these views do not necessarily reflect the actual activities of the IT department and the IT manager, they represent how the informants *perceived* how they worked with these issues. We found no examples of managers being involved in ISM-related problem solving/knowledge creation, analysis, storing, and retrieval in this more formal way.

When informants discussed their own area of expertise, on the other hand, there were strong representations of primary tasks (informants were happy to elaborate, were generally more animated, and provided far more details). The strong representations clearly make them better able to establish goals, identify gaps between goals and outcomes, formulate strategies, and generally make sense of their situation. When asked to discuss IS and ISM, informants primarily talked about high-impact, high-visibility incidents (e.g., computer theft, system breakdowns, viruses, and crises). This somewhat reactive learning orientation was evident when the impact of the natural disaster was discussed. The event engendered a most thorough review and documentation of the lessons learned, and interviewees were quick to relate their takes on IS to this process. This form of "flash learning" is not ubiquitous: Primary work tasks are embedded in a finely detailed web of concepts and indicators, including but not limited to the major events, that can be used as forward-looking planning instruments as well as retrospective evaluation tools. (Perceived) peripheral issues such as IS belong to a special category that will get isolated flashes of retrospective attention when something goes disastrously wrong. There is then a risk that single events—and subsequent analysis—will come to dominate learning and interpretation of related (in our case) IS risks.

Learning associated with IS and ISM lacks this elaboration, and the informants' approach to IS/ISM can best be described

as a form of sense-making (Weick, 1995) where managers extrapolate from something that is known and familiar in order to make sense of the less charted terrain of ICT and IS/ISM.

The implication for management is that narratives that provide meaning and a rationale for new policies and routines, and that connect to existing sense-making efforts in the organization, may be a crucial part in the early stages of creating awareness, as evidenced in this case.

Micro Track—An Interpersonal Outlook

The most obvious example of direct interaction and influence processes in this study is the way that the IT manager goes about his work. Most striking is his emphasis on the importance of continual interaction and relationship-building with employees on all levels, and his experience-based assertion that written policies alone will not resolve problems. This interpersonal style of influence—"management by walking around"—is promoted by another interviewee who argues that the live personal encounter is particularly important in a geographically dispersed organization where "management by mail does not work," as this interviewee tersely puts it.

The IT manager communicates the standards and norms as laid down in formal policies and rules, and then prepares to discuss and explain—at some length—why they make sense from technological, strategic, and security viewpoints. Through this process, both his fellow managers and other employees are provided time and opportunity to become aware of their own attitudes and, possibly, to adopt new ones. At the same time they learn about standards, goals, and relevant norms in the organization and develop their understanding of ICT in general and pertinent IS issues and the company's overarching take on ISM in particular. The opportunity for relaxed, informal dialogue enables employees to "manage themselves" and to participate in a process where they can develop awareness of risks and threats and learn how to deal with IS within their organizational role/task. It is this awareness and ability that can be perceived as making up the critical "coping skills at boundaries" that Rasmussen (1997, p. 191) refers to. An important point is that in order for managers to be able to support development of these skills in employees, they have to be guided by the kind of systemic understanding discussed in the macro track.

This kind of leadership in connection with ICT and ISM is seldom addressed in the literature, though there are exceptions. Enns et al. (2003) discuss how IT managers should eschew sheer pressure (which tends to generate resistance) and instead use rational persuasion and personal appeal in order to influence their peers more effectively. Albrechtsen and Hovden (2009) even consider relationships between ISM officers and other employees to be generally problematic and that this relational breakdown may widen into a "digital divide," separating users and information security managers, and hardening radically different, indeed incompatible, perspectives, to the detriment of the organization.

CONCLUSIONS

Linking Leadership to ISM: Advantages of the Three-Track Approach

At the start of this enterprise we set out to identify and discuss possible mechanisms by which managers may help or hinder the development of ISM in an organization. When exploring the mechanisms involved in how leadership influences awareness and implementation of ISM, we suggested that these mechanisms can be fruitfully analysed using three complementary tracks: cognitive/behavioral (micro track); learning and knowledge (meso track); and systems (macro track). The pilot study would tentatively seem to vindicate this proposition: It did not present much of a problem to anatomize the analysis of our empirical data in the suggested way. The tracks should prove helpful when analysts prepare to formulate hypotheses and specific (survey or interview) questions to guide interventions and experiments. This is a step toward a more structured theoretical understanding of how leadership can be linked by awareness to vital aspects of IS and ISM. Ultimately, the benefits should trickle down to individual ISM stakeholders, who get three very specific areas to analyze and strengthen in order to improve actual (rather than formal) implementation of IS.

Without such a guiding structure, it is easy to mistake "success" in one of the tracks for generally successful management of a complex issue area. A company may, for instance, have adopted a number of measures that have duly resulted in overall IS improvement. But if, on closer inspection, the measures all reside on one of our three levels, that should mean that there are still plenty of unexplored opportunities that management perhaps never even contemplated. Conversely, a general feeling that ISM is handled badly may well hide latent organizational strengths (e.g., management failure may be confined to one of the levels) to build on or complement.

An upgraded ability to identify more detailed strengths and weaknesses will thus, perforce, aid anyone interested in improving information security. The suggested approach also situates leadership and relates it to a number of well-known organizational practices (e.g., strategic planning; evaluation; various forms of accounting; use of performance indicators; etc.) in a way that acknowledges the inherently mediated character of work in contemporary organizations. Since this reflects how top-level actors in such organizations actually go about their business, there is little rubbing against the grain: Suggested strategic elements should not feel very alien, and should thus be fairly easy to accommodate.

While the development and demonstration of the theoretical framework are the main focus of this article, the case itself furnishes real-world insights how IS can be and, we suggest, often is perceived by key decision makers in an organization that adds to the stock of knowledge in this field. Albrechtsen and Hovden (2009) identified what they referred to as a digital divide between IS managers and users that could undermine the efficacy of policies and ISM implementation. The results from

the interviews in this study indicate that IS almost to a fault seems to be the exclusive domain of the CIO/IT manager, and that other managers mostly interpreted ICT and IS from their own areas of responsibility, or related it to very general security concerns. Such a divide within a company's management team may have far-reaching consequences for awareness and the quality of implementation efforts—particularly as we widen the perspective to include more than primarily technical approaches and checklists. As organizations become less tightly coupled and more complex, traditional management-by-directive models become less feasible. We argue that our framework demonstrates why general (i.e., non-IT) managers must play an active role vis-à-vis IS, and also, more specifically, how their actions may affect employee awareness, attitudes, and behaviors in ways that crucially facilitate implementation of ISM.

Generalizations from the demonstration case study should be done with caution. The company was selected because it was active in a business that was related to critical infrastructure and could be expected to have a relatively sophisticated approach to both safety and security issues. It was also profitable (meaning that it could easily afford relevant measures), had a good safety record, and was an active member in relevant national business networks. We see no reason to believe that this company would be any worse with respect to ISM than a typical enterprise, but given that this is a single case study, we cannot back up such a claim at this point. Ideally, this study should be followed by large-scale surveys and experimental studies where the efficacy of framework-derived interventions could be properly tested.

That said, a number of the general findings in this study echo findings that have been reported in a number of other studies: for example, that information security is rarely a top priority for managers; that the interest in information security is contingent on the role of ICT in the business the company is involved in (McFadzean et al., 2007); that many employees have a limited understanding of both IS risks and possible measures; that there are often considerable gaps between IS specialists' and general managers' understanding of IS (Albrechtsen & Hovden, 2009); and that the focus is often on technical solutions rather than on formal and informal measures (Sveen et al., 2009).

From Default Situation to IS Initiatives

Our study of an organization with a relatively under developed conceptualisation of IS throws light on what is probably the default situation in many organizations, and improves our understanding of the prevailing conditions before IS initiatives are embarked upon. A somewhat surprising finding was that IS was in fact a relatively alien concept to most informants and that they were so quick to refer to (a) the IT manager's expertise, (b) their own background and experiences (from their respective areas of expertise), and (c) the shared experience of a major event (disaster) that had affected the company in a serious way. Similar circumstances pertain to many (if not most) organizations where IS and ISM are generally perceived as relatively peripheral and alien issues, if not bothersome routines and limitations of personal autonomy (Albrechtsen, 2007).

This indicates that an IS initiative needs to address aspects of legitimacy, meaning, and sense-making to be successful. Different individuals and groups within an organization will typically make sense of IS based on their local area of expertise and on shared formative experiences. To kick off proper change, one would be well advised to connect to these specific sense-making resources (Weick, 1995). The first step for leaders may thus not be to "implement a policy" but to engage in preparatory dialogues that make sense out of the general role of ICTs in the organization, of IS, and of the possible benefits of ISM.

A notable recognition is that shared formative experiences, such as disasters, may indeed reduce or remove opposition to thorough review of fundamental work practices and thus prepare the ground for possibly radical organizational changes. However, a sufficiently potent event may "freeze" the process of making sense of events, and narratives, so that preparations to meet a similar event blind the organization to future dangers that do not fit the "benchmark catastrophe."

Somewhat paradoxically, the status of IS as a (perceived) marginal phenomenon may lead to learning processes of an assimilative nature, characterized by sense-making either based on familiar themes from work tasks or based on critical incidents—in both cases focusing on legitimacy that may in fact hamper implementation and true awareness.

Some Implications for the Practice of ISM

Ultimately the benefits of the analytical framework should trickle down to individual ISM stakeholders, who get three very specific areas to analyze and strengthen in order to improve actual (rather than formal) implementation of IS. Some tentative advice to practitioners in the field based on the findings of this study would be:

- Respect the fact that the various actors are unlikely to have a sophisticated or coherent notion of what IS actually is. Relate to experiences of well-known incidents and initially adapt accounts to fit the role of ICT in operations, as perceived by the actor, and his or her level of understanding of the issues. Early stages of IS implementation may, for instance, to some extent have to be introduced by a more general sharing of narratives and the subsequent gradual elaboration of more sophisticated IS sense-making.
- If managers are expected truly to support IS, ISM, and the development of information security awareness, they have to be able to draw on a shared understanding of ICT and IS and the macro (systemic) perspective, that is, to understand ICT and IS in relation to overarching strategy, structure, employee behavior(s), attitudes, and knowledge, over time. These are the mental models and understanding that we outlined in the

macro track, and the learning mechanisms belonging to the meso track.

- The next step is to have managers actively promote the organization's IS measures in their daily interaction with subordinates. This is where a genuine familiarity with IS matters and how they pertain to the organization writ large (as well as the local subsetting) becomes so important. If presentations of IS matters convey a sense that IS is a separate and only intermittently revisited concern, then that is basically what it will become.
- It is important to establish mechanisms that genuinely support evaluation and systematic learning from IS-related incidents. Since learning processes run the risk of being undermined by a lack of competence and interconnected defensive routines, this entails more than organizing events or devising information material where such matters are discussed. Ideal organizational learning mechanisms will facilitate critical thinking and constructive communication by being part of a comprehensive "learning plan" plan where aspects on all three levels (micro, meso, and macro) are considered.
- Technical measures, policies, and rules are important but have to be complemented by a level of awareness that can be improved through recurring interaction designed to change attitudes, norms, and competences—for instance, by using goal-setting and feedback loops.

REFERENCES

Alvesson, M., & Sköldberg, K. (2004). *Reflexive methodology. New vistas in qualitative research*. London, UK: Sage.

Ajzen, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology*, *52*, 27–58.

Ajzen, I. (2005). *Attitudes, personality and behavior*. Milton Keynes, UK: Open University Press.

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

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

Argyris, C., & Schön, D. (1996). *Organizational learning II. Theory, method, and practice*. San Francisco, CA: Addison-Wesley.

Bandura, A. (1997). *Self efficacy. The exercise of control*. New York, NY: W. H. Freeman.

Boisot, M. (1998). *Knowledge assets. Securing competitive advantage in the information economy*. Oxford, UK: Oxford University Press.

Boisot, M., & Li, Y. (2007). Organizational versus market knowledge: from concrete embodiment to abstract representation. In M. Boisot, I. C. MacMillan, & H. K. Seok (Eds.), *Explorations in information space. Knowledge, agents, and organization* pp. 109–146 Oxford, UK: Oxford University Press.

Burns, T., & Stalker, G. M. (1961). *The management of innovation*. London, UK: Tavistock.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Info Systems Journal*, *11*, 127–153.

Enns, H. G., Huff, S. L., & Higgins, C. A. (2003). CIO lateral influence behaviors: Gaining peers' commitment to strategic information systems. *MIS Quarterly*, *27*, 155–176.

Ferlie, E., Pettigrew, A., Asburner, L., & Fitzgerald, L. (1996). *The new public management in action*. Oxford, UK: Oxford University Press.

Hannah, S. T., & Lester, P. B. (2009). A multilevel approach to building and leading learning organizations. *The Leadership Quarterly*, *20*, 34–48.

Ilgen, D. R., & Davis, C. A. (2000). Bearing bad news: Reactions to negative performance feedback. Applied Psychology: *An International Review*, *49*, 550–565.

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

Kenney, M., & Florida, R. (1993). *Beyond mass production: The Japanese system and its transfer to the US*. Oxford, UK: Oxford University Press.

Kluger, A. N., & DeNisi, A. (1996). The effects of feedback interventions on performance: A historical review, a meta-analysis, and a preliminary feedback intervention theory. *Psychological Bulletin*, *119*, 254–284.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow D. W. (2006) The top information security issues facing organizations: What can government do to help? *Information Security and Risk Management*, *15*, 51–58.

Latham, G. A., & Locke, E. P. (1991). Self-regulation through goal setting. *Organizational Behavior and Human Decision Processes*, *50*, 212–247.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge, UK: University of Cambridge Press.

Lipshitz, R., Popper, M., & Friedman, V. J. (2002). A multifacet model of organizational learning. *Journal of Applied Behavioral Science*, *38*, 78–98.

Lundestad, C. V., & Hommels, A. (2006). Software vulnerability due to practical drift. *Ethics and Information Technology*, *9*, 89–100.

McFadzean, E., Ezingard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, *31*, 622–660.

Monge, P.R., Fulk, J., Kalman, M. E., & Flanagin, A.J. (1998). Production of collective action in alliance-based interorganizational communication and information systems. *Organization Science*, *9*, 411–433.

Neal, A., Griffin, M. A., & Hart, P. M. (2000). The impact of organizational climate on safety climate and individual behaviour. *Safety Science*, *34*, 99–109.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*, 14–37.

Oswick, C., & Robertson, M. (2009). Boundary objects reconsidered: From bridges and anchors to barricades and mazes. *Journal of Change Management*, *9*, 179–193.

Pawson, R. (2006). *Evidence-baced policy. A realist perspective*. London, UK: Sage.

Perrow, C. (1984). *Normal accidents. Living with high risk technologies*. New York, NY: Basic Books.

Polanyi, M. (1958). *Personal knowledge. Towards a post-critical philosophy*. London, UK: Routledge & Kegan Paul.

Powell, W. W. (1990). Neither market nor hierarchy: Network forms of organization. *Research in Organizational Behavior*, *12*, 295–336.

Rainer, R. K., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do information security professionals and business managers view information security issues differently? *Information Systems Security*, *16*, 100–108.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, *27*, 183–213.

Reddick, C. G. (2009). Management support and information security: An empirical study of Texas state agencies in the USA. *Electronic Government, An International Journal*, *6*, 361–377.

Rivard, R., & Lapointe, S. A. (2010). Cybernetic theory of the impact of implementers' actions on user resistance to information technology implementation. *Proceedings of the 43rd Hawaii International Conference on System Sciences—2010*, 1–10.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*, 31–41.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The DATA BASE for Advances in Information Systems*, *38*, 60–80.

Snook, S. (2000). *Friendly fire. The accidental shootdown of U.S. Blackhawks over northern Iraq*. Princeton, NJ: Princeton University Press.

Sundström, M., & Holmberg, R. (2008). The weakest link, human behaviour and the corruption of information security management in organisations—An analytical framework. *IMSCI '08: 2nd International Multi-Conference on Society, Cybernetics and Informatics, Vol. III, Proceedings*, Orlando, FL, June 29–July 2 (pp. 94–99). Retrieved from http://www.lu.se/o.o.i.s?id=12683&postid=1375206

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security. *International Journal of Critical Infrastructure Protection*, *2*, 95–109.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, *17*, 207–227.

Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected. Assuring high performance in an age of complexity*. San Francisco, CA: Jossey-Bass.

Yukl, G. (2002). *Leadership in organizations*. Upper Saddle River, NJ: Pearson Education.

Yukl, G. (2009). Leading organizational learning: Reflections on theory and research. *The Leadership Quarterly*, *20*, 49–53.

ABOUT THE AUTHORS

Robert Holmberg earned his PhD in psychology from Lund University (Sweden). He is currently Assistant Professor in Work and Organisational Psychology at the Department of Psychology, Lund University. His research interests include human resource management, leadership development, information security, implementation, and knowledge utilization.

Mikael Sundström earned his PhD in political science from Lund University (Sweden), and is currently Assistant Professor at that department. His main research interests include democratic theory and political communication, organization and leadership development, information security, and more generally the nexus between IT and the social sciences.