The Weakest Link Human Behaviour and the Corruption of Information Security Management in Organisations - an Analytical Framework

Sundström, Mikael; Holmberg, Robert

Published in:
IMSCI '08: 2nd International Multi-Conference on Society, Cybernetics and Informatics, Vol III, Proceedings

2008

The Weakest Link

Human Behaviour and the Corruption of Information Security Management in Organisations – an Analytical Framework

Robert Holmberg, Ph D
Department of Psychology, Lund University
Box 52, SE-221 00, Lund, Sweden

Mikael Sundström, Ph D
Department of Political Science, Lund University
Box 52, SE-221 00, Lund, Sweden.

ABSTRACT

In this paper we introduce the *norm-injection analysis framework*, a construct which can be employed to aid analysis of processes that affect information security management (ISM) in organisations. The underpinnings of this framework draw on – and evolve – theories about how apparently mundane organisational processes, particularly managerial demands on employees, may in some instances lead to undesired, perhaps calamitous, consequences. Because the mechanisms between input (demand) and the adverse consequences work by gradually accruing and multiplying subtle communication "problemettes" into major problems, they are almost undetectable to the untrained eye. Breaches of ISM protocol may appear wholly mysterious to the crash investigators brought in to analyse, post-event, what went wrong.

The norm-injection analysis framework is intended to shed light on these below-the-radar processes, and to supplement the tool set an organisation analyst has at his disposal when preparing or evaluating strategic ISM measures.

1. INTRODUCTION

It used to be easy. If you handle fire this way, you will get burnt. If you handle it this way, you will cause smoke to drift into the cave, making Mr. Flintstone dangerously unhappy. Knowledge was almost tangibly concrete, and could easily be passed from fire-keeper to fire-keeper. Do this and you will be secure; do that and you will be less secure.

Used to be easy, but is no longer. In a volatile and complex world, knowledge about security (among other things) is sometimes so ephemeral that it seems to dissipate even as you are absorbing it. To have someone memorise a particular sequence of button clicks that will "ensure security" ("trust me on this one, son") is obviously dangerous when there is a real risk that the panel holding those buttons may itself at any moment unceremoniously be consigned to the nearest landfill. More importantly, such an approach dulls the recipient's powers to understand, on a fundamental level, what security *is*, and to stay alert to future, hitherto unimagined threats.

To put the case succinctly: when it grows hard to pin down manifest and immutable threats, it becomes ever more important to foster *structural conditions* that engender and internalise watchfulness and resourceful handling of security-related information from pertinent sources (and an accompanying ability to appraise the value of those sources). Successful ISM, then, is in large part dependent on a sophisticated understanding *how* to foster beneficial structural conditions, and how the exercise of authority affect these processes, whether for good or bad. A guiding realisation, in the current effort, is that *any* form of assertive directive (however humdrum) will have structural repercussions that must be taken into proper account. In the following, we will attempt to map some such consequences, when we outline the *norm-injection analysis framework.*

2. THE PRACTICE OF ISM

Concerns about how to implement ISM in organisations have resulted in progressively more intense research activity. The research, however, often seems to be driven by very different and pragmatic problem formulations resulting in a field that suffers from notable fragmentation (Siponen & Oinas-Kukkonen, 2007). ISM implementation has been discussed in some recent contributions (Chang & Ho, 2006; Thomson & von Solms, 2006). The concept of organisational *culture* has recently been introduced to the ISM-field (Vroom & von Solms, 2004; Chang & Lin, 2007) and more specifically for risk management of ISM (Tsohou, Karyda & Kokolakis, 2006). There is a sizable general literature dealing with diffusion and implementation from a variety of angles (Rogers, 1995; Holmberg & Fridell, 2006). Karyda, Kiountouzis & Kokolakis (2005) studied processes of formulation, implementation and adoption of security policies in two public service organisations. Their findings indicated that organisational structure, management support, an appointed security officer and awareness programs, all contribute to successful implementation (ibid.). Other examples of studies relating to behaviour or human factors explore how different groups perceive security issues in different ways (Rainer, Marshall, Knapp & Montgomery, 2007).

3. FROM MINDLESS TO MINDFUL ISM

In a recent paper, Thomson and von Solms concluded that the highest mode of ISM realisation is "information security obedience" (Thomson & von Solms: 2006). We think that this conclusion is spectacularly mistaken, and concur with Neal, Griffin and Hart (2000), when they venture that an organisation's safety

performance is *not* only a reflection of its members' compliance – "adhering to safety procedures and carrying out work in a safe manner" ((ibid., p 101) – but that it is also heavily reliant on their level of "safety participation", defined as "helping co-workers, promoting the safety program within the workplace, demonstrating initiative, and putting effort into improving safety in the workplace" (ibid.).

This notion, that safety (and in our case security management) is something that is not only managed (*compliance*) but also can be viewed as something that one *participates* in, is pivotal to our argument in this paper. In fact, we will suggest that the issue of IS participation is likely to be a crucial aspect when trying to come to terms with IS and adopting ISM in organisations. When reducing employees' ISM role(s) to one of mere compliance, opportunities to reflect on both ISM contribution options and on factors that may limit the implementation and long term impact of ISM-measures are effectively curtailed.

A focus on compliance/obedience necessitates a strict technocratic perspective that, by definition, excludes more sophisticated analysis of how knowledge, work processes, relations within and between groups and values/norms interact with dictated standards and policies. Organised study of still more fundamental issues related to surveillance, privacy, integrity and legal and psychological contracts between employees and employers is similarly relegated to the sidelines.

In addition to this explicit emphasis on participation in a wider sense, we find it important to elaborate somewhat on the concept of *mindfulness*. Weick and Sutcliffe (2001) define mindfulness in the context of high-reliability organisations as: "a combination of ongoing scrutiny of existing expectations, continuous refinement and differentiation of expectations based on newer experiences, willingness and capability to invent new expectations that make sense of unprecedented events , a more nuanced appreciation of context and ways to deal with it, and identification of new dimensions of context that improve foresight and current functioning" (p. 42). In contrast to mindfulness they discuss mindlessness in the following way: "When people function mindlessly they don't understand either themselves or their environments, *but they feel as though they do*. They feel that because they have routines to deal with problems, this proves that they understand what's up…Whenever a routine is activated, people assume that the world today is pretty much like the world that existed at the time the routine was first learned. As with most expectations, people tend to look for confirmation that their existing routines are correct. And over time, they come to see more and more confirmation based on fewer and fewer data. What is missing are continuing efforts to update the routines and the perceptions, expectations, and actions that accompany them" (Weick & Sutcliffe, 2001, p. 43).

While compliance or obedience can in many cases be realised by following strict rules to the letter, more flexible behaviour and adaptation to new situations depend on more refined understanding of the issues at hand. In a study of implementation of new safety regulations within the nuclear industry, Marcus (1988) found that units with poor safety records tended to implement new routines in a rule-bound or "mindless" fashion, while units with a good record tended to adapt the routines to fit their local situation.

This condensed review indicates that while there is a fast growing literature on how to implement ISM and the role of organisational culture, values, leadership and so forth, there is a need for a perspective that incorporates the employee or the individual as a proper actor and that takes work processes and knowledge seriously. To this end, we suggest that further research should benefit from incorporation of concepts such as:

- Information security *participation* rather than compliance/obedience
- Information security *mindfulness*
- *Work processes* and how they interact with ISM
- ISM as an integral process of *knowledge creation*

In order to develop models to guide research and actual implementation and evaluation, these concepts have to be integrated within a framework specifying their internal relations and how they are eventually to be made operational in real-world studies. In the next section we outline the rough contours of just such a framework.

4. INTRODUCING THE NORM-INJECTION ANALYSIS FRAMEWORK

It is easy to see, then, that a set of psychosocial factors is at the heart of the outlined problem. It is just as easy to see that we need to prepare solid analytical tools even to approach such all-encompassing yet non-specific complications –"psychosocial factors" is, to put it mildly, not a readily employable concept.

Fusing a number of communication-centric theoretical strands, we now introduce a coherent *norm-injection analysis framework* (NIAF) which is explicitly engineered to detect problems – and opportunities – when a collective is presented with authoritative demands to alter aspects of its knowledge management. As we shall see, it may not even be clear to the authority that posed directives (which may on the surface of things seem comfortably concrete and limited in scope) can have such wide-ranging repercussions. A distinct benefit of a model such as the one we are proposing is that it helps illuminate such obscured features.

We begin with the collective, and how its knowledge management may be conceptualised. We then introduce an external "injector" entity able to influence the collective, and thus to affect the collective's "idea management" routines. The contextual embedding of the collective – i.e. how it is situated in a larger organisational setting – is likely to affect its resilience against external injection, and the framework provides relevant parameters to assimilate such differences. Norm injection is finally unlikely to be a one-off affair. Instead the recursive dynamics between "injector" and "injectee collective" must be taken into account. After all, in the face of observed resistance, the external actor is likely to react in order to ensure subsequent norm injection success.

5. STEP ONE: THE COLLECTIVE AND THE SOCIAL LEARNING CYCLE

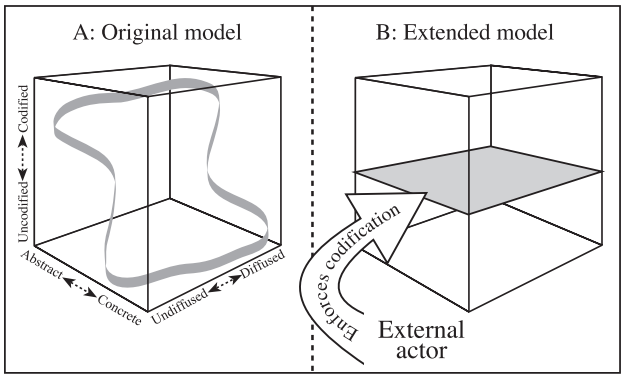
Let us start with the conceptualisation of the collective itself. Boisot (1998; 1999) has modelled collective knowledge creation and management as a *social learning cycle* (SLC). Using three fundamental dimensions, *codification, abstraction and*

diffusion, he visualises a perpetual cycle taking place within an imaginary dimensional box (figure 1 (A)).

As long as we stay in the realm of abstract modelling, the *size* of the box (i.e. which actors are included in it) is of negligible consequence as its archetypal characteristics remain fundamentally unaffected. When we eventually pave the way for real-world analysis, things change. At some point we need to be able to locate the collective and its boundaries, while acknowledging the undeniable fact that an organisation comprises many nested and partly overlapping "boxes", each with its idiosyncratic set of embedment characteristics.

In practice, we will be looking for telltale signs of a *community of practice* rather than for a "department", a "group" or an "organisation". Etienne Wenger (who coined the term together with Jean Lave) defines communities of practice as: "…groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly" (Wenger, 2008). Such a definition would imply that a community of practice in many cases can be regarded as a potential or an ideal, rather than a fully realised form. Gherardi and Niccolini (2000, p. 10) argue that it is "conceptualised by various authors as an informal aggregate defined not only by its members but also by the shared ways in which they perform their work and interpret events…". Crucially, members of a community of practice are usually able to identify its reach, and actors which are emphatically "external" in a community of practice sense (that this is important will soon be made evident).

Figure 1: The SLC Model, Basic and Extended



Codification refers to the extent that knowledge can be expressed in an economical and formalised way. "..the number of bits of information required to carry out a given data processing task" (Boisot 1998, 46). "[T]he more completely one codifies a task, the more one effectively fossilises it…Complete codification, then, allows a task to be performed entirely by machine without human intervention" (ibid. 47).

Abstraction refers to the degree of conceptualisation, stretching from concrete, here and now, irreducible experiences to highly abstract, generalisable formulations concerning regularities and cause and effect-relationships. "If codification allows us to save on data-processing resources by allowing us to group the data of experience into categories, abstraction allows us to realise further savings in data processing by minimising the number of categories that we need to draw on for a given task" (ibid. 49).

Diffusion refers to how many actors that are exposed to or have access to a certain form of knowledge. "…the proportion of a given population of data-processing agents that can be reached with information operating at different degrees of abstraction" (ibid 52).

6. STEP TWO: THE SLC COLLECTIVE AND EXTERNAL ACTORS

Boisot's original focus does not compel him to differentiate between various actor groups. We find it a useful extension to separate in-box "true SLC" actors from external entities who have the power to enforce dimensional restrictions by edict. These are managers and external consultants with authority to decide how a particular problem or thought complex is to be framed.

The very identification with a certain collective or a group has been shown to contribute to escalating conflicts and negative attitudes towards outgroups. A useful analytical approach for the analysis of this kind of dynamics is social identity theory (Ashforth & Mael, 1989). This has general bearing on how outgroup requests are received by a collective. Here, however, we are interested in how demands affect SLC dimensions and by extension, the SLC itself.

Enforcement of codification, for example (figure 1 (B)), might involve strict definitions of the codes/language used to identify security-related issues. Issues which do not fit this language risk turning invisible, or becoming subsumed under mismatching headings (more on this soon). This is challenge enough, but in an abstract sense the fundamental problem is that the SLC, that holding pattern of complex human knowledge generation and regeneration, risks becoming stunted, resulting in unpredictable, potentially malign, longer-term consequences.

Figure 1 (B) admittedly depicts an extreme case of codification "closure", but external actors can hardly avoid interfering with SLC parameters when they are exercising their authority. Such out-box actors thus always need to weigh potential SLC impact against the utility and absolute needs to impose uniformity in any of the three dimensions.

We have elsewhere expounded on the perils of SLC stunting (Sundström & Holmberg 2008). In brief these include impeded (group) powers of creativity and innovativeness; potential psychosocial problems in the workplace; loss of "tacit" experience-based knowledge; erection of patterned thought-structures, including barriers, and more (table 1 lists a *very* simplified summary of dimension characteristics).

We believe that retarded SLC dynamics can help explain why edicts from "outside" often fail to take root properly in specified settings. In-box actors intuitively recognise that their "natural" learning cycle is not working properly, and proceed to distance themselves from it, by establishing alternative, informal structures and systems beyond management's direct control.

Table 1: Brief Dimensional Summary

		Information management aspects (examples)	Fields of practice (examples)	Adverse human consequences (examples)
Codification	High	Set alternatives (tick boxes) in data management tools	Software achitecture	Sense of frustration as model does not fully reflect reality, and assault on own value systems
	Low	Open (free text) fields; non-set alternatives	The Arts, Thinktanks, Design	Sense of frustration at the lack of unobtrusive controls, and set tasks
Abstraction	High	Information represented and communicated through formal, quantitative models	Science, engineering (i.e. symbolic work)	High demands on educational and cognitive capacity; captures a "slice" of reality
	Low	Information represented and communicated through narratives, examples and cases	Nursing, child care (more or less essential component in most practices)	Time-consuming, difficult to test, may be prejudiced and authoritarian
Diffusion	High	Information and knowledge is diffused and widely shared, open for use	Writing, using word processors and the internet	(at extreme end) Overwhelming cognitive capacity
	Low	Information and knowledge is isolated to a few locations	Brain surgery, design of word processors and internet-based search engines	Chasm between laypersons and experts

7. THE DARK SIDE OF THE FORCE: INTERCONNECTED SLC SECTORS

Let us elaborate this final point, which is pivotal. We have so far envisaged a "white sector" SLC where extant information is accessible to both SLC members and, at least nominally, to external entities. It is this SLC that may be subject to edicts from the outside. It is basically possible for the external authority to declare how a given idea complex is to be codified, abstracted and diffused – and thus risk *stunting* the white sector SLC, with often unpredictable, sometimes undesirable, consequences. One consequence is this. Like life in Jurassic Park: when there is life there is a way. As the white sector SLC is squeezed by managerial demands, a black sector appears to restore "lost" aspects of the SLC and circumvent intrusive demands (as SLC collaborators see them). Crucially, such black sector idea management is much harder to pick up and make sense of by external actors. Checks may seem to indicate that management demands are being followed – the sanctioned protocols of language and codes are being dutifully observed, roughly as decreed, in official data management systems. Yet around the water cooler and in the office cubicles other terminology is being used. A colleague decides to keep a useful ledger to record experience-based findings that do not fit the provided evaluation forms (codification). A novel term is invented to approximately denote a set of common and related work tasks and it gradually becomes ubiquitous except – on pain of upbraiding – when discussing formally with management (abstraction).[1] A helpful postit-note explains how password X can be used to bypass those obnoxious security checks to get the printer going (diffusion). And so on.

[1] Mismatching assumptions what term X actually implies may lead to the complete failure to carry out a particular sub-task, while still in effect reporting that it has been completed.

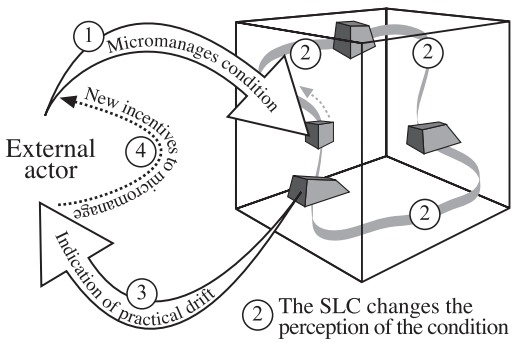
This is paradoxical: the very exercise of authority with the aim to impose SLC "order" risks driving processes and knowledge creation and storage underground *to where authority cannot easily reach*. Authority may thus lead to *less* authority; decreed streamlining of knowledge management may lead to *less* streamlined knowledge management. Because the white-to-black sector transferral process is itself so hard to catch, and because actual black sector SLC processes provide no formal "storage & analysis stations" but are (haphazardly) diffused throughout the collective, there is in practice a continual and invisible drift from projected ideals. The meshed kludge – to put it harshly – of black and white SLC processes is likely to work reasonably well in most circumstances (imploding organisations would otherwise be a tediously common occurrence). The first detection of the steadily widening rift between ideal and practice may in fact be catastrophic system failure – failure that the original edicts may very well have been designed to forestall.

8. STEP THREE: RECURSIVE DYNAMICS AND PRACTICAL DRIFT

Once we introduce the external actor, we thus need to account not only for what may happen within the SLC, but also elaborate on the ongoing dynamics between the external actor and the SLC-collective – including the recognisably real issue of practical drift we just discussed.

Snook (2000) has made an important contribution here when he studied incidents of friendly fire, and what actually caused these lethal chains of events. He uncovered numerous problems based on group characteristics, and a variety of psychological inhibitors that acted to restrict the efficiency of issued orders as well as adherence to standardised operating procedures. Much simplified, practical drift can, in Snook's conceptualisation, be defined as noted aberration between original intentions, as decided and injected by some external authority, and subsequent audits (by the same external authority) of on-the-ground realisations of those very intentions. There is, in Snook's view, a risk that such practical drift triggers attempts to revise the instructions and make them yet more detailed in order to overcome noted "interpretation deficiencies". This solution may in fact aggravate the problems if intrinsic organisational deficiencies are left untouched, while the amount and complexity of the instructions gradually increases (figure 2). Interesting, to us, is that practical drift is easy to merge with the extended SLC model, further enhancing its capacity to address a complex set of issues. Let us again consider figure 2:

Figure 2: SLC and Practical Drift



The figure models practical drift in relation to the extended SLC, where (1) represents an actual norm injection attempt. The core of practical drift is, in fact, nothing *but* the untrammelled SLC gradually morphing input to alleviate the incorporation of knowledge in existing knowledge structure(s) –and relate it to already existing data. The trouble is that because much of this SLC in fact resides in the black sector, it takes a long time for the external actor to get any sort of indication that the meticulously designed instructions have somehow been (possibly fatally) perverted. When indication comes, it is, we repeat, likely to be sudden and shocking – maybe the result of investigation into a major system failure. This discovery almost inevitably leads to frenzied activity aiming to restore and further fortify original instructions: to squeeze out undesired alterations to original concepts. After all, it is easy to surmise that uncovered breaches of protocol are the culprits, rather than *how the protocol was designed and/or promulgated in the first place*.

Unless action is taken carefully to mould and temper fundamental SLC dynamics – not rout them – and to nurse black sector SLC components back into the white sector where they are in plain view, the problem is likely to perpetually repeat itself.

9. PLANNING AND ANALYSING SLC NORM INJECTION

We now finally prepare to move one step up from abstract modelling towards, if not yet all the way to, real-world analysis. We stress that it is both possible and desirable to develop a range of analytical superstructures to be attached to the NIAF undercarriage. We are about to outline the contours of one such possible superstructure, and while it certainly has intrinsic value, it is also a way to show *how* the NIAF may be thus extended. We would avidly welcome more efforts of this nature. Ajzen and others (Ajzen, 2001; Francis et al., 2004a; 2004b) have developed a trisected *theory of planned behaviour* that offers a stringent way to study communication aspects on the individual level that have implications for security compliance or the more mature *participation* and *mindfulness*.[2] It has been used in hundreds of empirical studies and must thus be considered conceptually much more evolved than constructs like organisational "climate" or "culture".

An obvious allure is that this theory provides a NIAF-compatible conceptual apparatus that can be of great help in a real-world analysis. The Ajzen (2001) theory specifies three "variables" which predict behavioural intentions:

1) *attitudes* towards specific behaviours (including beliefs about the consequences of the behaviour and evaluation of the outcomes, i.e. does the person think that they good or bad?)

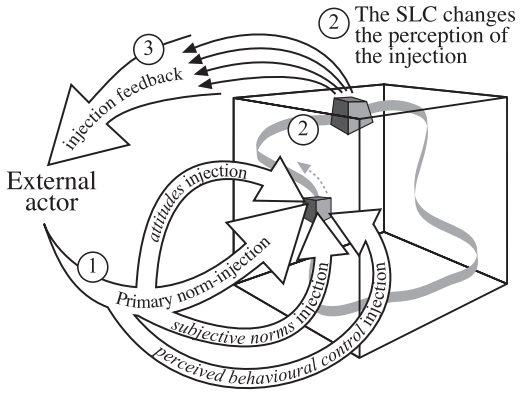
2) *subjective norms*, i.e. beliefs about how other persons and groups want the person to behave and the person's evaluation of these norms/pressures

3) *perceived behavioural control* which concerns the degree of control over a certain behaviour and the degree of ability to perform the behaviour (self-efficacy)

[2] The focus is on individual antecedents to behaviour with relevance to IS. studying *changes* in those antecedents over time provides us with an attitudinal and intentional individual psychological correlate to organisational processes like practical drift and social learning cycles.

We basically argue that if the external actor makes a real effort to integrate these three aspects into norm-injection attempts, it is less likely that the SLC runs away with the concept(s). This is because members are provided with a new way to triangulate understanding of the edicts, both internally and when interacting with colleagues. This triangulation and the thus established linkages reinforce original norms, and slows evolution (or "decay" as the injector would probably have it) caused by SLC processes.[3] Scheduling early feedback sessions it might be possible to note deficiencies in these "support injections" – and then do something about it – nipping the problem in the bud, rather than waiting for it to bloom.

Figure 3: The NIAF and the Theory of Planned Behaviour



10. COLOUR ON THE CANVAS – THE GOOD, THE BAD AND THE NORM-INJECTION ANALYTICAL FRAMEWORK

Although we have outlined several "problems" along the way in order to illustrate specific points, we now need to furnish more organised normative guidance related to the various framework components. We basically believe that it is possible to attach generic worse/better legends to the various abstract benchmark dimensions we have introduced. We should then be able to formulate normative propositions to act as a bridge between abstract theory and concrete investigation.

It should be noted that the specific empirical setting where we employ the NIAF affects the relative *weight* of the normative assertions – even though the assertions themselves stay valid. For presentational purposes, we have so far evoked a situation where external actor demands grate against the "natural" SLC of the influenced collective. Clearly, this will aggravate whatever problems a NIAF analysis will expose. Just as clearly, it is possible to envisage far more harmonious settings, where problems are light to the point of inconsequentiality. This said, we think that ISM in most settings will typically exhibit genuine grating characteristics. Outside of organisations where security is in some sense "in the blood" (e.g., security consultants, military organisations, the police and so on) ISM will of necessity-include demands that are alien to, and thus interfere with, (perceived) primary work tasks. This will in turn almost inevitably

[3] This structural focus is also how we stay true to NIAF priorities. Theoretical candidates for NIAF "superstructure-remodelling" may have many interesting uses, but NIAF compatibility hinges on the capacity to process and/or predict *structural* impact.

generate a level of resentment… and grating. The following sample of propositions is formulated with such an ISM context in mind,[4] even though it has relevance well beyond it.

- The extent to which employees behave in ways that support an organisations information security policy is determined by the individual's: 1) attitude to the behaviour, and beliefs and attitudes toward the outcomes of the behaviour, 2) the individual's perception of norms concerning the behaviour and finally 3) the extent to which the individual believe that he or she has control over the behaviour and is able to perform the behaviour.

- Sustainable and flexible ISM is characterised by participation and mindfulness and depends on open and legitimate processes of learning and knowledge creation (SLCs) within relevant communities of practices.

- Implementation of IS-systems that in their form structure SLCs in ways that restrict or stunt them lead to a less open, shared and legitimate process (pushing SLC into the dark sector).

- When SLCs become less open, shared and legitimate they will contribute to processes of practical drift that under conditions of tight coupling will lead to major errors, incidents etc.

- External actors will tend to address signs of practical drift by further specification of rules and routines (micromanagement) in a way that in most cases further undermine the SLC.

- When external actors take the SLC into account and the form and content of ISM implementation explicitly support an open, shared and legitimate SLC, employees will behave in a participative and mindful way in relation to IS.

- Taking SLC and the structural conditions into account incorporates both a design that support those attitudes, norms and competencies that support participation and mindfulness as well as the structuring of abstraction, codification and diffusion of the SLC

10. RE-FORGING THE WEAKEST LINK

We have striven to indicate that the weakest link in ISM is not the individual, nor his or her bounded powers of reason or cognitive capacity. Nor is it the collective *per se.* Instead we direct attention to collective knowledge management functions, and structural implications for these functions when external actors attempt to inject altered norms into the collective. We believe that *this,* the injection phase, is the weakest link in ISM. Once a new norm successfully takes hold, and not just in a superficial or lip-service sense, the chain grows stronger again.

Coming to terms with the weakest link – reforging it – involves developing sophisticated strategies to minimise SLC damage when exercising authority. It means threading with extreme care, and be vigilant to signs that a black sector is taking over SLC functions. It means continual and proactive monitoring of how concepts and ideas are altered in the SLC – and sometimes embrace those changes and alter other parts of the system to take them into official account.

[4] These propositions, and others, are slated for empirical testing in an ongoing project where communities of practice that vary in their degree of ISM success will be used to design valid measures of the different concepts in the framework. The ultimate objective is to develop an empirically grounded model that can guide analysis, implementation and evaluation ISM with focus on learning cycles and so forth.

LITERATURE

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

Ashforth. B., & Mael, F. (1989). Social identity theory and the organization. *Academy of Management Review*, 14, 20-39.

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

Boisot, M., & Cox, B. (1999). The I-Space: a framework for analyzing the evolution of social computing Technovation 19, 525–536

Chang, S.E., & Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106Pzz(3), 345-361

Chang, S.E., & Lin, C-S. (2007). Exploring organizational culture for information security management. Industrial Management & Data systems, 107(3), 438-458.

Francis, J. F., Eccles, M. P., Johnston, M., Walker, A., Grimshaw, J., Foy, R., Kaner, E.F.S., Smith, L., & Bonetti, D. (2004). *Constructing questionnaires based on the theory of planned behaviour. A manual for health service researchers*. REBEQI project. Retrieved from http://www.rebeqi.org/ViewFile.aspx?itemID=212

Francis, J. F., Johnston, M., Eccles, M. P., Grimshaw, J., & Kaner, E.F.S (2004). *Measurement issues in the theory of planned behaviour. A supplement to the Manual for constructing questionnaires based on the Theory of Planned Behaviour*. Retrieved from http://www.rebeqi.org/ViewFile.aspx?itemID=219

Gherardi, S., Nicolini, D. (2000). The organizational learning of safety in communities of practice. *Journal of Managament Inquiry,* 9, 7-18.

Holmberg, R., & Fridell, M. (2006): *Implementering av nya behandlingsprogram i kriminalvården.* Kriminalvårdens forskningskommitté. Rapport 20. (http://www.ewenger.com/theory/)

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

Marcus, A. M. (1988). Implementing externally induced innovations: A comparision of rule-bound and autonomous approaches. *Academy of Management Journal. 31,* 235-256.

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

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? Systems Security, 16,

Rogers, E. (1995). *Diffusion of innovations (4e uppl.).*London: The Free Press.

Siponen, M. T., & ; Oinas-Kukkonen, H. (2007) A Review of Information Security Issues and Respective Research Contributions. *Database for Advances in Information Systems,* 38, 1; ABI/INFORM Global pg. 60

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

Sundström, M., & Holmberg R. (2008). Paradigm Petrification in the Information Age. An Anatomisation of Knowledge Creation and Deliberation in Innovation Systems in the Human Services. Submitted to Public Administration Review

Thomson, K-L., & von Solms, R. (2006). Towards an information security competence maturity model. *Computer Fraud and Security*, May, 11-15.

Tsohou, A., Karyda, M., & Kokolakis, S. (2006). Formulating information systems risk management strategies through cultural theory. Informnation Management and Computer Security, 14, 198-217.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. Computers & security, 23, 191-198.

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