View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2009 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2009

Addressing The Human Factor In Information Systems Security

Peter Bednar
University of Portsmouth, peter.bednar@ics.lu.se

Vasilios Katos
Democritus University of Thrace, vkatos@ee.duth.gr

Follow this and additional works at: http://aisel.aisnet.org/mcis2009

Recommended Citation
Bednar, Peter and Katos, Vasilios, "Addressing The Human Factor In Information Systems Security" (2009). *MCIS 2009 Proceedings*. 72.
http://aisel.aisnet.org/mcis2009/72

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

ADDRESSING THE HUMAN FACTOR IN INFORMATION SYSTEMS SECURITY

Bednar, Peter, University of Portsmouth, Portsmouth PO1 3HE, UK and Lund University, Sweden, peter.bednar@ics.lu.se
Katos, Vasilios, Democritus University of Thrace, Xanthi 67100, Greece, vkatos@ee.duth.gr

Abstract

In this paper the historically persistent mismatch between the information systems development and security paradigms is revisited. By considering the human activity systems as a point of reference rather than a variable in information systems security, we investigate the necessity for a change in the information systems security agenda, accepting that a viable system would be more user-centric by accommodating and balancing human processes rather then entertaining an expectation of a one sided change of behaviour of the end user. This is done by drawing upon well established information systems methodologies and research.

Keywords: *Information Systems Security, Information Systems Methodologies, Contextual Analysis, User Controlled Design*

1 INTRODUCTION

There is an emerging need in ISS (Information Systems Security) to recognise the human factor as a security enabler rather than an obstacle. ISS has to be dealt with as context dependent as opposed to context independent. This means that ISS cannot be an add-on but has to be an intertwined aspect of any IS (information system) design effort and change practice. The reason why it is treated in many cases as an add-on is because ISS is confused with data systems security. Recent events indicate that it is becoming increasingly obvious that data security processes cannot be built on models which ignore real world organizational behaviour. If necessary, organizational activities require people to circumvent and bypass even fundamental data security practices in their professional struggle to do their jobs those security processes could never fulfil their intended function. Security processes which are modelled outside of the real world organizational context are prone to antagonize effective organizational practices and the literature maintains a plethora of such real world cases. A representative case is UK's HM Revenue and Customs Department where a junior official sent two CDs containing personal data of families receiving child benefit to an office in London, by unregistered courier services (BBC, 2007). Furthermore the pervasiveness, penetration and commercial success of laptops have amplified the number of security incidents as the assumption of physical security is challenged. A high profile incident was the case of the Royal Navy recruiting officer in Birmingham, UK, whose laptop was stolen as he decided to bypass the security procedures and carried a laptop with unencrypted data (BBC, 2008).

When it comes to addressing the human aspects of security, a substantial proportion of the relevant ISS literature focuses on user awareness and education. Although the importance of security education perhaps can not be stressed enough, it does not address some of the most important issues of human aspects of security systems such as relevance in context and motivation. Undoubtedly a user would need training and his or her behavior towards the system will differ when compared to a system with no (technical) security. The system in turn should also consider and accommodate the user's security requirements. This is commonly referred to as usable security (Cranor & Garfinkel, 2005), which also relates to an attempt to conjunct the apparently opposing terms of security and usability (Gedda, 2006, Gutmann & Grigg, 2005). For the purposes of addressing the human factors in ISS, concerns about stakeholder motivation and contextual relevance have to be included to accommodate suitable behavioural change in organisations. It is

argued in this paper that there is a compelling need to move on from the idea of usable data system security or ISS onto the idea of useful ISS.

The rest of this paper is structured as follows. In Section 2 relations between ISS and IS methodologies are presented. In Section 3 issues emerging from analysis and design approaches are outlined. In Section 4 paradigmatic influences are introduced as relevant to developing an understanding of contextual dependencies. In Section 5 motivation is presented and justified to serve as a key to addressing human factors. This is presented as part of the foundation for accommodation of ISS. Finally, Section 6 presents the conclusions.

2 RESEARCH IN INFORMATION SYSTEMS SECURITY

Although there is a wide consensus in the IS community that security should be incorporated in the complete IS analysis, development and implementation process, systematic and systemic treatment of systems analysis and development with elements of ISS seemed to exhibit some belatedness. Siponen (2005) attempts to study this by considering the background of the information scientists and security researchers in the context of the different disciplines involved. More specifically he draws a distinction between IS, software engineering, computer science and mathematics and associates the different research communities with the mentioned disciplines. As such, researchers in the area of computer science and mathematics have a positivist orientation, whereas researchers in IS often subscribe to the interpretive paradigm. Software engineering though incorporates both interpretivism and positivism since this discipline inherits ideas from social sciences (Sharp, Robinson & Woodman, 2000).

Irrespective of the separation between computer science and software engineering, it appears that the crucial factor that had an impact on the inclusion (or exclusion) of security practices in IS methodologies was the interpretivism vs. positivism view. For example in the commonly available academic reference work on Information Systems development by Avison and Fitzgerald (2003), the poor reference to security overall is very pertinent. This problem is just as recognizable in professional references such as the BCS (British Computer Society) reference on Business Analysis by Yeates et al (2006). While ISS is not inherently excluded it is contextually taken for granted (e.g. not made explicit). As such inexperienced analysts, developers and organizational change agents may trivially neglect the ISS dimension. Explicit ISS appears to fall mainly under the computer science discipline (usually positivist with an inherent focus on artefact development), strongly coupled with mathematics approaches (such as cryptography for example). A conceptual approach focusing on rational and formal descriptions leads work intended to cater for ISS in practice to almost solely focus upon data systems security. Therefore the result would tend to be developed independently of the needs of the surrounding human activity system. Unfortunately, ISS is dependent on human motivation and behaviour within the stakeholder context. This conceptual and paradigmatic mismatch explains the language espoused where people talk about “educating the user”; “train the user”; “make the user follow proper security procedures”; “change user behaviour to more secure ones” and so on. It ignores the fact that as change is required from the user the system as a whole (human activity system) obviously was either not designed at all explicitly but as a result of unintended consequences of data system security design. Basically the security aspects of the system were inappropriately “designed” in the first place (otherwise changing behaviour to specifically incorporate ISS would not be necessary). The problem with requiring people to change behaviour is that any professional activity is dealt with in an effective way due to some contextually relevant reason. To request people to change behaviour is to try to change organizational practices without understanding the effective behaviour of the involved stakeholders in the first place (lack of compatibility between the real behaviour of professional stakeholders and any requested formal changes are likely to lead to security failures in context). Information systems people on the other hand, primarily engaged within the interpretivism's realm, have welcomed Information Systems Auditors whose functions are mainly interpretive based. As auditing is an activity that is typically

incorporated once a system is rolled out (or perhaps during a testing phase), it is of no surprise that security activities were limited during the early stages of the system lifecycle (or focus on risk analysis). Tryfonas et al. (2001) proposed an interpretive framework for expanding and incorporating the security functions in the whole IS development. Although the interpretive approach could have been anticipated and would certainly be appropriate for such an exercise, it seems that a positivist direction needs at some stage to be questioned and researched. It should be noted that this research question is not dealt with in this paper, but the authors felt that it needs to be mentioned for the sake of completeness.

Rather than researching into the creation of new methodologies and models for information systems and security, we argue that it would be more useful to consider ways of incorporating security thinking into the existing IS methodologies, adopting the view by Tryfonas et al. (2001). We argue that a monolithic secure systems development methodology would be of limited value to IS. ISS functions are dependent on both human and infrastructural elements of an IS and should not be considered in isolation from each other. Furthermore, the IS field has a long history of addressing research questions in multidisciplinary contexts – such as systems thinking, structuring uncertainty, defining and managing wicked problem spaces, (Langefors, 1966; Checkland, 1981; Mumford et al, 1985; Hirschheim and Klein, 1989; Friis, 1991; Nissen et al, 1991; Myers, 1994; Langefors, 1995; Checkland and Holwell, 1998; Ciborra, 2002; Mumford, 2003; Whitaker, 2007) to name a few – and ISS should benefit from such experience and practices. Therefore when it comes to considering the security aspects of the human activities in a system, it seems reasonable and beneficial to do this through the prism of IS. We argue that a systemic view of security would result to a number of desirable states:

- system analysts and organisational stakeholders would have a better understanding and view of security issues in situated practices to perform contextually relevant risk analysis;
- security controls and features would be created and exist intrinsically as part of the development process as both creative possibilities and constraints which would not need to be unconsciously bypassed by organisational stakeholders within their professional work. This situation would lead to a robust system;
- organisational stakeholders (“end users”) would not only have a better understanding of the role and application of the security functions, but also would be able to contribute to more contextually relevant processes and within the system as security controls.

3 ANALYSIS AND DESIGN OF THE SECURE SYSTEM

Against the above, we can look on IS methodologies that have purposely incorporated ISS aspects. As security analysis is closely coupled with risk analysis, the CRAMM methodology (UK's Central Computing and Telecommunications Agency's Risk Analysis and Management Method) is a widely used risk analysis methodology. CRAMM has for example been studied and discussed by Dhillon and Backhouse (2001) in conjunction with IS development methodologies such as SSADM (Structured Systems Analysis and Design Method and Business Development Method; e.g. OGC, 2001). Downs et al. (1992) studied the “compatibility” between SSADM and CRAMM and identified ways that CRAMM could effectively tap into any stage of SSADM, whereas Baskerville (1993) proposed an interface in detail between CRAMM and SSADM. McDermott and Fox (1999) expanded the UML concept of use cases to include security incidents of abuse case models, later to be referred to as misuse cases. Since then a number of researchers promoted the idea of misuse cases, and developed methodologies and templates for capturing misuse cases. Although the concept of the misuse case model is a neat way to describe some attacks to the system, there are fundamental and important aspects that have been overseen:

- one of the main purposes of a use case model is to specify the boundaries of the system to be studied, analysed or implemented. Under this view, a system is sought to be closed.

Consequently, one can be led to the false assumption that the set of misuse cases is complete and there are no other possible ways to attack the system;

- a use case describes business activities which at some point could be translated into a set of functional specifications. A misuse case does not fit this purpose;
- to the best of our knowledge, there is no misuse case in the literature showing an association between a legitimate actor and an adversarial actor. This association should be labelled as "social engineering". Provided that the human is usually the weakest link in the security of an IS, and that many attacks exploit and misuse trust relationships, it can be seen that this is an important and potentially dangerous omission;
- a misuse case model, at its current stage, is not capable of capturing and describing successful impersonation (identity fraud) attacks, as in that event it would not be possible to distinguish a use from a misuse case. In other words, if an attacker assumes the identity of a legitimate actor, the case model would not have any means for identifying this state of the system;
- misuse cases distract the (security) analyst from the factors that contribute to high risk, simply because these factors are outside the use cases box.

The weaknesses in CRAMM are however similar to weaknesses in SSADM which have been criticized and questioned for many years within the IS field (e.g. in the work of Peter Checkland, Enid Mumford, Frank Stowell, Hans-Erik Nissen; Borje Langefors as mentioned above and others). The issues surrounding the criticisms relate to the naive understanding of scientific paradigms including a confused understanding of what an Information System might be defined as. In the field of IS contextual adaptation is recognized as necessary to dynamic organisational practices in complex environments. It has been acknowledged for example that it is beneficial to conceptualize IS as a Human Activity System, which according to Checkland is a very different problem arena from viewing IS as a data processing system (Checkland, 1981; Checkland and Holwell, 1998; Checkland and Poulter, 2006). There is a visible confusion when it comes to assumptions about systems, which is noticeable when discussing the purpose of "best practice" (e.g. to implement best practice vs. to learn from descriptions of best practice and to develop your own). This highlights the difference between the standardized system and complex system assumption (e.g. even standardized technological systems are uniquely placed and used due to contextual dependencies in organizational situations – the human activity systems are never the same). We do not wish to confuse simplification such as "good enough analysis" with the typical idea referring to 80 percent of the problem solved as if it would by some magic automatically mean that "the relevant problem" has been solved. The problem with misjudging a problem space described with being by default the relevant problem space to engage has been discussed thoroughly by Peter Checkland. He has also demonstrated several times in his work that one of the most difficult aspects in System Analysis and Development is the questioning and reframing of any problem space presented. Context and relevance is a discussion also related to the phenomena of confusing individually specific threats with statistical risk / threat. Basically you could not assess the danger for any one particular person out of context only on the basis of generic statistical evidence. In this paper we address the problem of the human oriented, human focused IS design with an emphasis on ISS.

Do any ("interpretatively" based) IS methodologies deal with ISS? This is not a simple question and the answer is complex and paradoxically a yes and no. Holistic IS methodologies support analysis into any relevant aspect of IS analysis and development. Methodologies such as SSM (Soft Systems Methodology) by Peter Checkland (1981) and ETHICS (Effective Technical and Human Implementation of Computer supported Systems) by Enid Mumford (2003) deal with complex organizational issues and this could indeed include security if the analysis team chooses to do so. We argue that the result is dependent on the competences of those analysts and stakeholders involved. However from the point of view of the paradigm espoused behind those holistic methodologies all method applications is by definition applied by analysts and stakeholders so the outcome would

always depend on the specific human actors involved. Any outcome would not be determined by the choice of method, as methods do not apply themselves independently of human involvement and subjective interpretation. Traditionally, holistic and systemic methodologies have successfully been applied in a multitude of uncertain and complex organizational problem spaces for the last forty years or so (see for example descriptions in Nissen et al, 1991; Langefors, 1995; or overview in Avison and Fitzgerald, 2003). The issue is however that methodologies in general do not specifically highlight or guide the user in ISS. ISS is not specifically highlighted with any great detail or discussed and problematized in the leading reference works as part of IS methodologies. It could be argued that this is a feature of systems thinking as the holistic approaches generally do not specify details uniquely. Those issues that are relevant in context and important to deal with would be discovered in a holistic and thorough analysis. But there is a problem inherent in that people have now implemented technologies, which they have very little historical experience of in context and are therefore likely to be unfamiliar with the resulting security implications. ISS processes are alien to the professional organizational members ("end user's") point of view, as they do not necessarily understand the implications on ISS as a result of their contextually relevant professional behaviour. ISS processes are also alien to the security expert point of view, as they do not necessarily understand the locally situated and contextually dependent relevant (work) processes or the necessity of application of ("end user's") professional judgement and behaviour in situated context. Complex problems require professional problem solving activities to be treating problems in context as unique instances and so not un-problematically in accordance with some prescribed recipe (method or systematically applied process of inquiry and development). Therefore formal descriptions of professional practice would by definition be erroneous. To request and demand people to ultimately follow protocols is to sabotage the possibility for professionals to effectively apply their personal competence and judgment of situation and issue. The result is not only an inhuman organisational monster but furthermore a suicidal organisational monster as it defies the fundamental principles of Ashbys law of requisite variety (Ashby, 1956) making the organisation incapable to adapt to its environment.

There have been efforts to apply specific security methods, methodologies and standards (see for example the ISO 27001 standard, the body of knowledge regarding systems auditing by ISACA, 2009, and NIST, 2002, risk management guide, where security methods, standards and protocols, model behaviour is secured). But these are generally speaking structured, formalized and systematic. They focus on formal behaviour and actions of organisational members. As such it is predictable that the logical human behaviour and the real world professional practices are being ignored. To develop models of human behaviour based on description of organisational activity will have little real world significance as can be seen through the history of IS development failures. Basically the fundamental flaws in the application of structured and formal methods in traditional IS methodologies such as SSADM are bound to be repeated in ISS methods if the efforts ignore lessons learned from real world organisational analysis, development and change. A very possible attitude in organisational behaviour is that security issues are turned a blind eye to. It is possible that in many organisations it is not acceptable to highlight security threats. People may not "want to know", some will experience comments on weaknesses in security as comments on their personal competence. To highlight security threats brings with it several organisational, social and cultural dangers. People could find themselves accused of being a security threat, e.g. "if you had not mentioned the security threat it would not have been known and therefore not a problem". This kind of phenomena means that there are real organisational incentives not to discuss or make an effort to prove any threat as that in itself would by definition be a breach of security and the employee might not be treated well as a result. On one hand people are ignored and security issues are ignored through a practice of denial (there "is no threat"); and on the other hand any effort to prove the point that a threat indeed exist is culturally and social ostracized and expressively antagonized by definition from a management perspective. This leads to unwillingness to highlight (especially from grass root level perspective) real security threats. People's unwillingness to admit and highlight real security threats could be justified

by the introduction of regulatory controls and compliance which attempts to remedy this issue to some extent. For instance, the so called SOX compliance which involves a mandatory security certification according to the Sarbanes-Oxley Act (GPO, 2002) in the US and affects all US companies listed on the stock market, requires companies that have suffered from security breaches to inform their stakeholders and customer base. Naturally this requirement had an impact on the management layers of the corporate as well as the employees.

By failing to appreciate the complex relationships between use, usability and usefulness, the security procedures imposed are not only subject to possible misuse but they are likely to be a core hindrance to everyday legitimate work.

When talking about usability analysts are mainly drawing upon HCI (Human Computer Interface) related aspects. This however is a discourse with difficulties as for example usability in HCI is not necessarily equal to usefulness in IS research. This is especially true in the context of viewing IS from an interpretative point of view such as the Scandinavian and British Schools of IS thinking (e.g. Enid Mumford, Peter Checkland, Hans-Erik Nissen et al, 2007; and many more). Usefulness in IS is not necessarily focusing on usability of an artefact. Focus on artefact use does not engage with contextual relevance of meaningful application as part of everyday work practices in purpose outside of the specified role of the artefact (e.g. intended use situation vs. real world situations). For example to rigorously focus on achieving usability attributes, usability properties to be designed into the product or system is not the same as to focus on what makes use of a particular artefact relevant in specific contexts and situations (as in common exceptions). Inherent in user interface design is focus on designing a nice product (I am pleased with it etc); easy to use product (to create an understanding of how to use it does not require a lot of effort); nice function (to recognize features of the product in a positive “feel-good” fashion); usability (to be able to use the product and to understand what the products does). So there is a difference between good quality usability properties and the relevance of the product use in particular, specific and possibly changing contexts (Yes I know how it works; yes it is nice; yes I like it; yes it is pretty; yes it does something great; yes it does something I want it to do in my job; yes, yes, yes as answers to all questions – but no I am not actually using it in my job… - because it is not appropriate in my situation at the moment).

Security procedures may interfere with perfectly reasonable, and from a professional stakeholder point of view necessary, processes in practice and specific contexts. Indeed formal adherence to bureaucratic processes is traditionally seen as the best way to undermine any effective organisational behaviour. The weakest link is not necessarily in the (technical) system itself but the difference between the formal model of usage and real usage of system content (data) as such in a human activity system.

Design of use in context is not only about ways of advancing end user’s motivation in keeping with proposed policies and assuming the necessity of applying them, but also about the designer’s understanding of advancing their own motivation and efforts in re-evaluating the promoted (security) policy. This (promoted security policy) may be experienced by affected stakeholders as contextually necessary to ignore (for them to be able to do their job properly). Similar issues have already been dealt with in holistic IS methodologies such as ETHICS by Enid Mumford (2003), Soft Systems Methodology by Peter Checkland (1981), Client Led Design by Frank Stowell (Stowell and West, 1994), Object Oriented Analysis and Design by Lars Mathiassen et al (2000) and approaches such as the SST (Strategic Systemic Thinking) framework by Bednar (2000). The multitude of IS definitions continue to haunt efforts in development of IS related efforts (e.g. discussions in Mumford et al, 1985; Hirshheim and Klein, 1989; Nissen et al, 1991; Langefors, 1995; Checkland and Holwell, 1998; Bednar, 2000; Nissen et al, 2007; Klein and Myers, 2009). Some effort to deal with this can be viewed in the discussion on information security versus ISS by Karyda et al. (2001). The IS definition (IT vs IS) on security influences what the practical aim on the security focus is. It is quite obvious when taking human activity systems into consideration that IS security must be a build-on (e.g. part of systems analysis and organisational change) and not an add-on (reflective measures

focused mainly on protection of existing data systems). Historically we could argue that to for example anticipate a loss of the availability of the underlying system is well catered for in holistic and systemic methodologies such as those mentioned above. What is historically not engaged with in any depth or in an explicit way is support for a client led design of ISS. Thus ISS failures could often be attributed to a mismatch between formal models of systems and the real world human activity system. To ignore the complexities and contextual dependencies of human activity system (e.g. to confuse it with a formal rational model of a human activity system) will not only make the formal system irrelevant and flawed but it will also undermine ISS.

4 IGNORANCE OF METHOD AND PARADIGMATIC ISSUES

For years there have been IS professionals and academics that have mixed and matched aspects of different holistic and systemic methodologies. People have combined ideas from methodologies within both the same paradigm as well as across different paradigms. In the description of SSADM, for example, the methodology itself is in complex situations recommended to be combined with both SSM and / or ETHICS. Software engineers are recommended (e.g. Sommerville, 2007) to engage with methodologies such as SSM and ETHICS when dealing with complex organisational problems (as opposed to stick to their normal formal techniques used for artefact design and project management). Some (like the authors of this paper) have critically revised features from holistic methods (such as SSM and ETHICS) to support the local creation of contextually relevant systemic approaches. It is not as if this effort has not been done before. Ultimately though we have yet to find much evidence of a discussion among practitioners and academics which incorporates and explicitly embraces these manifestations in available narratives and texts. There is of course no reason for why methodological support for the creation of contextually relevant approaches would not include concerns specific to ISS. The purpose of methodologies is from our point of view not a naïve belief that they would ever be applied. We advocate that the purpose of a methodology (narrative) is a pedagogical one to guide and help the analyst in their efforts to discover and create a competent way forward. Particularly for the less experienced analyst or for engagement in novel context it could be experienced as a "life-saver". Methodologies are not about teaching people how to "do analysis". They are about supporting people in their own discovery and creation of contextually relevant processes.

In Mumfords ETHICS analysts have support mechanisms and descriptions with advice, comments and examples for over twenty different but related analyses. In Checklands SSM there is also numerous support for complex analysis with the promotion of a multitude of concepts and techniques (such as CATWOE, PRQ, Rich Pictures etc). In the Stowells Client Led Design different methods and techniques from SSM expanded upon and new ones added (such as PEARL etc). In Mathiassens et al's OOA several techniques from methodologies such as ETHICS and SSM are transformed, changed and incorporated with an object oriented focus (with tools such as the FACTOR analysis for example). The SST framework by Bednar includes several techniques and modelling support for analysis especially aimed at inquiries into uncertain and complex problems spaces (incorporating para-consistent logic, techniques for structuring uncertainty from multiple systemic perspectives and including techniques for modelling diversity networks etc). Additionally these methodologies include critically informed discussions supporting the problematization of the analytical process and enquiry. There would appear to be good opportunities to enhance such methodologies with both guiding techniques focusing on ISS as well as expanding the cover and focus of existing techniques to incorporate explicitly ISS concerns. Additionally the critically informed process of inquiry could incorporate specific ISS features.

5 MOTIVATION

Professional competence is dependent on factors which are both internal and external to the organisation at hand. Individuals' actions are interdependent with rewarding (re)actions by other individuals (see for example discussion by Bateson, 1972; 2002). Socio-cultural relation and exchange processes are inherently emotionally grounded (internally rewarding or punishing) and not only rational and explicit (Churchman, 1968; 1979; Bateson, 1972; 2002; Lawler, 2001; Ciborra, 2000; 2002). Motivation to highlight security issues as unintended consequences of organisational change (including the result of implementation of processes intended to promote data security), is heavily dependent on extra role behaviour. Individual behaviour may not be directly recognised by the formal reward system (Organ, 1988). Extra role behaviour cannot be viewed as universally expected (to exist in organisational practices) as by definition lack of extra role behaviour is not normally a reason for negative consequences (see for example discussion by Van Dyne et al 1998). However two categories of extra role behaviour could be recognized as having direct consequences for the development of ISS (e.g. "helping" and "voice" behaviour). Individuals helping others even when there is no formal requirement of their job is categorized as "helping behaviour". Individuals making efforts to propose change in formal requirements and processes is categorized as "voicing behaviour". Both of these categories of behaviour are inherently relevant and important in a complex organisational context where there is a necessity to facilitate improvement (Neneth et al 1989). Helping behaviour is often experienced as positive and supportive in organizational environments because it focuses on collaboration. Unfortunately "voicing behaviour", albeit necessary, is often experienced as challenging and negative (rocking the boat). It is often thought of as negative because it focuses on (and requires) a willingness for behavioural change (Van Dyne, 1998).

Satisfactory ISS perhaps needs to be recognized as means to give an organisation a "competitive advantage" rather than a compliance chore. For this purpose the development, and not only implementation, of security procedures may need to be co-designed by the actual stakeholders and users in the real human activity system where they are supposed to be applied (to avoid the creation of a competitive disadvantage; e.g. as opposed to suffer from, security procedures which are a hindrance to professional stakeholders work, or from failures by design and become the focus of organisational ISS scandals and so on) To stay competitive organisations are dependent on their embracement of existing creativity and sponsorship of the creation of new ideas and knowledge within their remit (e.g. Argyris, 1990; Weick, 1995; 1998; Oldham and Cummings, 1996). The organisational sponsorship of creativity has been recognized as a strategic choice specifically dependent on organisational context and management behaviour (Argyris, 1990; Weick, 1995; 1998; Shalley et al. 2000; Shalley and Perry Smith, 2003; Mumford et al. 2002). We argue that successfully implemented strategies and resolutions for ISS are inherently dependent on competence and knowledge of the situated work context. Situation dependency and contextual complexity and dynamics make it unsuitable to assume ideas of rational behaviour (commonly referenced to von Neumann and Morgenstern, 1944; Arrow, 1951 etc). The rational model for organisational problem resolution practice is unsatisfactory ever since the foundation for any assumption of complete analytical knowledge of future developments was refuted by the acknowledgement of open systems thinking; the works of Langefors (1966; 1995), Bateson (1972; 2002), Churchman (1968; 1979), Argyris, 1990; Weick, 1995; 1998; Ciborra (2000; 2002), Klein and Myers (2009) etc are representative of this paradigm. People have developed a recognition that organizational behaviour due to real world dynamics and complexities does not inherently comply to a rational or formal model (Bateson, 1972; 2002; Churchman, 1968; 1979; Argyris, 1990; March and Simon, 1958; Lindblom, 1959; March, 1978; or Baskerville and Land, 2004; etc.). As such any problem space is unequivocally intertwined with the unique problem solving activity of the specific professional stakeholder working in the organisational context in focus. To facilitate the development of relevant measures in context will require them to be (co-) developed by the stakeholders in context (e.g.

Mumford 2003; Checkland 1981; Friis, 1991; Stowell and West 1994; Mathiassen et al, 2000; Bednar 2000).

The assumptions related to a formal, rational bureaucratic model is thus full of issues and this includes a dysfunctional paradigmatic belief (for research into this phenomena see for example work by Selznick, 1948; Merton, 1949; Gouldner, 1954: Mintzberg, 1979; Bateson, 1972). A similar evolution of multiple parallel dysfunctional paradigms is also visible in discussion not only in a practitioner led world of IS development but also in IS research. More specifically, IS research where positivist approaches, rational models and closed systems thinking continue to live on even though both interpretative and critical approaches have been inherent key features in the IS academic field ever since its official inception as a specific area of interest at the IFIP conference in New York in 1965 (see for example discussion by Langefors, 1995). Complex and dynamical problem spaces put demands on organisational ability to be flexible and effectively to develop and continuously evolve their ability to re-organise. Organisational change and transformation is inherently characterized by political and cultural aspects (e.g. Mintzberg, 1979). The consequences of any IT and IS development efforts are very contextually dependent (e.g. discussions in Langefors, 1995; Checkland and Holwell 1998; Bednar 2000; Orlikowski and Iacono, 2001; Rogers, 2003; Baskerville and Land, 2004) and this would inherently also be the case with regards to ISS efforts.

The relation between organisation and IT has been discussed mainly under three perspectives. First, the role and function of IT in organisational environments has been discussed. The focus in this perspective is put on IT effectively. The attention is mainly on business strategy, infrastructure, technology architecture and investment in IT services (e.g. Earl and Feeny, 1994; Rockart et al. 1996; Broadbent and Ktizis, 2005). Second, the alignment between organisation and IT has been discussed. The focus in this perpsective is placed on IT strategy and formal business process reorganisation (see for example Zmud, 1988; Rockart, 1988; Keen, 1991; Willcocks et al., 1997; Orlikowski and Barley, 2001). The third perspective is that of stakeholder participation and control which heavily feature co-development, co-design and co-creation. (Langefors, 1995; Mumford, 2003; Checkland and Poulter, 2006; Stowell and West, 1994; Friis 1991; Bednar 2000 etc). The first and second perspectives above are usually discussed from within an inherently positivist paradigm. The consequential experiences, dissatisfaction with and critique of applications of a naïve positivist perspectives have been a main cornerstone in the works representing the third perspective mentioned above (see also for example Mumford et al. 1985; Boland and Hirschheim, 1987; Mumford, 1991; Nissen et al., 1991; Orlikowski and Baroudi, 1991; Checkland and Holwell, 1998 etc).

The relationship between the behaviour of individual organisational members and their use of technology has been discussed from mainly two different perspectives (see for example the discussion in Markus and Robey, 1988). On one hand there is the “Technological Imperative perspective” which is when technology use is considered as a result of technology determining behaviour (technological determinism). By being mainly based on a positivist paradigm, the focus is on implementing technological solutions and infrastructures as it is assumed that people will by default use technology (for intended purposes) once it is available to them. Stakeholders need to be educated and usability issues are also taken into consideration where use of technology is assumed to be a “natural’ consequence only dependent on availability and usability. On the other hand there is the “Emergent Perspective” which is when technology use is determined by the result of individually interpreted social interactions in a cultural context (DeSanctis and Poole, 1994). Use and adoption of technology is an emergent result of socio-cultural processes, availability of technology and individual contextual dependencies. Participation type and level of stakeholder engagement are directly linked to individual ability and motivation (see for example discussions by Mumford, 2006). This is influenced by the relationship between individual stakeholder and organisational culture, group culture and leadership style (such as autocratic versus democratic). Leadership style tends to be a factor with significant influence, where democratic leadership style supports the development of motivation for stakeholder participation and sponsors incentives for new ideas to surface.

Autocratic leadership on the other hand tends to inhibit the expression of new and unpopular ideas (e.g. Friis, 1991; Stowell and West, 1994; Checkland and Holwell, 1998; Mumford, 2006). Deterministic approaches to organisational consequences are problematic from many perspectives. An increase in task complexity also increases the demand for enhanced participation (e.g. Galbraith, 1978). Organisational change is not a matter of technology implementation (e.g. Euske and Roberts, 1987; Locke and Schweiger 1979) and this would also be the case for ISS. Contextual dependencies influence organisational members behaviour more than rational models and formalized security processes. The conclusion is that it is necessary to move on from a dominant (mainly positivist) paradigm in ISS efforts and agendas onto a more critically informed but inclusive interpretative one.

6 CONCLUSIONS

The involvement of the IS community in the ISS problem area is not necessarily a match made in heaven. The reason is that although it is at the core of the IS field and significant work has been done over the years the interpretative paradigm continues to be largely ignored by a vast part of the IS community. So much so indeed that Ciborra (2000; 2002) described the field as positivist and with a rational view of knowledge. This would include decision making and discussions about strategy and systematically created formal models of (closed) systems (complex or not). Ciborra expressed a wish to contribute to a transformation of the field towards inclusion of mood, passion and recognition of contextual dependencies (appreciated through for example improvisation). To motivate stakeholders Ciborra developed characteristics of what is put attention on in participatory design.

Klein and Meyers (2009) talk about the reciprocal relationship between IS research and IS analysis and development. They discuss criteria relevant for IS research vs approach to IS analysis and development. With a reference to Etzioni (1968) and others, the agenda for relevant interpretative and critically informed action (and research) is set. Fundamental criticism is necessary to develop an opportunity to provide new resolutions to complex social problem areas. The established communities-of-assumptions need to be challenged and alternative ones provided. However this does not require that all intellectuals agree with each other. It does require a significant effort by individual stakeholders (researchers or practitioners) to break away from a naïve positivist paradigm. It is our conclusion that it is of uttermost importance that efforts in ISS to be contextually relevant must engage contextual dependencies from a critical perspective. What Klein and Meyers (2009) describe as an explicit critique and improvement of social condition for the purpose to develop richer meanings and understanding and fundamentally to entice people to speak or not.

References

Argyris C. (1990). *Overcoming Organizational Defenses: Facilitating Organizational Learning*. New Jersey: Prentice Hall.

Arrow K.J. (1951). *Social Choice and Individual Values*. New York: Wiley 2nd ed. printed 1963.

Ashby, R. (1956). *An Introduction to Cybernetics*. London: Chapman & Hall.

Avison D. and Fitzgerald G. (2003). *Information Systems Development: Methodologies, Techniques and Tools*, 3rd edition, London: McGraw-Hill.

Baskerville, R. (1993), Information systems security design methods: implications for information systems development'', *ACM Computing Surveys*, 25(4)

Baskerville R. and Land F. (2004). Socially self-destructing systems. in Avgerou C., Ciborra C. and Land F. (Eds.), *The Social Study of Information and Communication technology: Innovation, Actors and Contexts*. Oxford: Oxford University Press.

Bateson G. (1972). *Steps to an Ecology of Mind*. University of Chicago Press.

Bateson G. (2002). *Mind and Nature: a Necessary Unity*. 5th edition. Hampton Press.

Bednar P.M. (2000). A Contextual Integration of Individual and Organizationl Learning Perspectives as part of IS Analysis. *Informing Science Journal*. 3(3), 145-156.

BBC, 2007. *Brown Apologises for records loss*. http://news.bbc.co.uk/1/hi/uk_politics/7104945.stm
BBC, 2008. *More MoD laptop thefts revealed*. http://news.bbc.co.uk/2/hi/uk_news/politics/7199658.stm
Broadbent M. and Kitzis E.S. (2005). *The New CIO Leader*. Boston: Harvard Business School Press.
Checkland P. (1981). *Systems Thinking, Systems Practice*. Chichester: Wiley.
Checkland P. and Holwell S. (1998). *Information, Systems and Information Systems*. Chichester: Wiley.
Checkland P. and Poulter J. (2006). *Learning for Action*. Chichester: John Wiley and Sons Ltd.
Churchman C.W. (1968). *The Systems Approach*. Dell Publishing.
Churchman C. W. (1979). *The Systems Approach and its Enemies*. Basic Books.
Ciborra C. (2000). *From control to drift: the dynamics of corporate information infrastructures*. Oxford: Oxford University Press.
Ciborra C. (2002). *The labyrinths of information: challenging the wisdom of systems*. Oxford: Oxford University Press.
Cranor, L. F. & Garfinkel, S. (editors) (2005). *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly.
DeSanctis G. and Poole M.S (1994). Capturing the complexity in advanced technology use: Adaptive Structuration Theory. *Organisation Science*, 5, 121-147.
Dhillon, G. & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11, 127–153.
Downs, E., Clare, P. and Coe, I. (1992), *SSADM: Application and Context*, Prentice±Hall, Englewood Cliffs, NJ.
Earl M.J. and Feeny D.F. (1994). Is your CIO adding value? *Sloan Management Review*, 35(3), 11-20.
Etzioni A. (1968). *The Active Society: A Theory of Societal and Political Processes*. New York: The Free Press.
Euske N.A., Roberts K.H. (1987). Evolving Perspectives in Organisation Theory: Communication Implications. in Jablin F.M., Putnam L.L., Roberts K.H. and Porter L.W. (Eds.), *Handbook of Organisational Communication: An Interdisciplinary Perspective*. New York: Sage Publications.
Friis S. (1991). *User Controlled Information Systems Development: problems and possibilities towards Local Design Shops*. Lund: Lund University Publications. Information and Computer Science.
Galbraith J.R. (1977). *Organizational Design*. Reading: Addison-Wesley.
Gouldner A.W. (1954). *Patterns of Industrial Bureaucracy*. New York: The Free Press.
GPO (2002). U.S. Government Printing Office. *The Sarbanes-Oxley Act of 2002*. Available from: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf
Gedda, R. (2006). Security vs. usability: No one's winning. *Computerworld*, October 11. Available from: www.computerworld.com.
Gutmann, P. & Grigg, I. (2005). Security Usability. *IEEE Security & Privacy*, July/August, 64-66
Hirshheim R. and Klein H.K. (1989). Four paradigms of information systems development. *Communication of the ACM*, 32(10), 1199-1216.
ISACA, (2009). Information Systems Audit and Control Association, Certified Information Systems *Auditor Review Manual*.
ISO/IEC, (2005). *Information technology - Security techniques - Information security management systems – Requirements.* International Organisation for Standardisation, ISO/IEC 27001:2005.
Karyda, M., Kokolakis, S. and Kiountouzsi, E. (2001). Redefining Information Systems Security: Viable Information Systems. *Proceedings of the 16th IFIP International Conference on Information Security* (SEC 2001), M. Dupuy, P. Paradinas (Eds.), 453-467.
Keen P.G.W. (1991). *Shaping the Future: Business Design Through Information Technology*. Boston: Harvard Business School Press.
Klein H.K. and Meyers M.D. (2009). A set principles for conducting and evaluating critical field studies in information systems. *Working paper*.
Langefors B. (1966). *Theoretical Analysis of Information Systems*. Lund: Studentlitteratur.

Langefors B. (1995). *Essays on Infology: Summing up and planning for the future*. Lund: Studentlitteratur.
Lawler E.J. (2001). An affect theory of social exchange. *The American Journal of Sociology*. 1007(2), 321-352.
Lindblom C.E. (1959). The Science of Muddling Through. *Public Administration Review*. 19(2), 79-88.
Locke E.A. and Schweiger D.M. (1979). Participation in decision-making: one more look. in Staw B. and Cummings L.L (Eds.), *Research in Organisational Behaviour*, vol. 1. 265-339. Greenwich: JAI Press.
Mathiassen L., Munk-Madsen A., Nielsen P.A., and Stage J. (2000). Object Oriented Analysis and Design. Aalborg: Marko.
March J.G. and Simon H.A. (1958). *Organizations*. New York: Wiley.
March J.G. (1978). Bounded Rationality, Ambiguity, and the Engineering of Choice. *Bell Journal of Economics*. 9(2), 587-608.
March J.G. (1991). Exploration and exploitation in organizational learning. *Organization Science*. 2(1), 71-87.
Marcus M.L. and Robey D. (1988). Information Technology and Organisational Change: Causal Structuring Theory and Research. *Management Science*, 34, 583-598.
McDermott, J., & Fox, C. (1999). Using abuse case models for security requirements. *Proceedings of the 15th Annual Computer Security Applications Conference* (ACSAC).
Merton R.K. (1949). *Social theory and social structure*. New York: The Free Press.
Mintzberg H. (1979). *The Structuring of Organizations: a synthesis of the reseaarch*. Englewood Cliffs: Prentice-Hall.
Mumford E., Hirschheim R., Fitzgerald G. and Wood-Harper T. (Eds.) (1985). *Research Methods in Information Systems*. New York: North-Holland Publishers.
Mumford E. (2003). *Redesigning Human Systems*. London: IRM Press.
Mumford, M.D., Scott, G.M., Gaddis, B. and Strange. J.M. (2002). Leading creative people: orchestrating expertise and relationships. *Leadership Quarterly*, (13), 705-750.
Myers M.D. (1994). A disaster for everyone to see: an interpretative analysis of a failed IS project. *Accounting, Management and Information Technologies* 4(4), 185-201.
Myers M.D. (1997) Qualitative Research in Information Systems. *MIS Quarterly*, 21(2), 241-242.
NIST (2002). *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology, Special Publication SP-800-30.
Nissen H.E., Klein H.K, and Hirschheim R. (Eds.) (1991). *Information Systems Research: Contemporary Approaches and Emergent Traditions*. The Netherlands: Elsevier Science Publishers B.V.
Nissen H-E., Bednar P. and Welch C. (2007). *Use and Redesign in IS: Double Helix Relationships?* Santa Rosa: Informing Science Press.
OGC (2001). *Business Systems Development with SSADM*. Office of Government Commerce (OGC). TSO (The Stationery Office).
Oldham G.R. and Cummings A. (1996). Employee creativity: personal and contextual factors at work. *Academy of Management Journal*, 32.
Organ D. W. (1988). *Organizational citizenship behaviour: The good soldier syndrome*. Lexington Books.
Orlikowski W.J. and Barley S.R. (2001). Technology and Institutions: What can research on Information Technology and research on Organizaions learn from each other? *MIS Qurterly*, 25(2), 145-165.
Orlikowski W.J. and Iacono C.S. (2001). Desperately Seeking the 'IT' in IT Research - A Call to Theorizing the IT Artifact. *Information Systems Research*. 12(2), 121-134.
Rockart J.F. (1988). The Line takes the Leadership - IS Management in a Wired Society. *Sloan Management Review*, 29(4), 57-64.
Rockart J.F., Earl M. and Ross J. (1996). Eight impratives for the new IT organization. *Sloan Management Review*, 38(1), 43-55.
Rogers E.M. (2003). *Diffusion of Innovations*. New York: The Free Press.

Siponen, M. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization* 15 (2005) 339-375

Selznick P. (1948). Foundations of the theory of organizations. *American Sociological Review*, 13(1), 25-35.

Shalley, C.E, Gilson, L. and Blum T. (2000). Matching creativity requirements and the work environment: effects on satisfaction and intntions to leave. *The Academy of Management Journal*, 43(2), 215-223.

Shalley C.E. and Perry Smith J.E. (2003). The social side of creativity: a static and dynamic social network perpsective. *Academy of Management Review*, 29.

Sharp, H., Robinson, H., & Woodman, M. (2000). Software engineering: community and culture. *IEEE Software*, 17(1, Jan.-Feb.), 40-47.

Sommerville I. (2007). *Software Engineering*. 8th edi. Harlow: Pearson Education.

Stowell F. and West D. (1994). *Client-led design: A systemic approach to information systems definition*. London: McGraw-Hill.

Tryfonas, T., Kiountouzis, E., Polymenakou, A. (2001). Embedding security practices in contemporary information systems development approaches. *Information Management & Computer Security*, 9(4), 183-197

Von Neumann J. and Morgenstern O. (1944). *Theory of Games and Economic Behaviour*. Princeton University Press. 2004 Reprint.

Van Dyne L. and LePine A.J. (1998). Helping and voice extra-role behaviour: Evidence of construct and predictive validity. *Academy of Management Journal*. 41, 108-119.

Weick K.E. (1995). *Sensemaking in organizations*. Thousand Oaks: Sage.

Weick K.E. (1998). Improvisation as a mindset for organisational analysis. *Organisation Science*, 9(5), 543-555.

Whitaker R. (2007). Applying phenomenology and hermeneutics in IS design: A report on field experiences. in Nissen H-E., Bednar P.M. and Welch C. (Eds.) *Use and design in IS: Double helix relationships?* Informing Science Press.

Willcocks L.P., Feeny D. and Islei G. (Eds.) (1997). *Managing IT as Strategic Resource*. Berkshire: McGraw-Hill.

Yeates D, Paul D, Jenkins T, Hindle K. and Rollason C, (2006). *Business Analysis*. BCS, British Computer Society.

Zmud R.W. (1988). Building Relationships Throughout the Corporate Entity. in Elam J.J., Ginzberg M., Keen P.W.G. and Zmud R.W. (Eds.), *Transforming the IS Organization*. Washington DC: ICIT Press.