The Case for Improvisation in Information Security Risk Management

Kennedy Njenga[1], Irwin Brown[2],

1 Department of Business IT, University of Johannesburg; Tel: +27 11 559 1253 email: knjenga@uj.ac.za
2 Department of Information Systems, University of Cape Town: Tel: +27 21 650 2677 email: irwin.brown@uct.ac.za

Abstract. Information Security (IS) practitioners face increasingly unanticipated challenges in IS risk management, often pushing them to act extemporaneously. Few studies have been dedicated to examining the role these extemporaneous actions play in mitigating IS risk. Studies have focused on clear guidelines and policies as sound approaches to ISRM (functionalist approaches). When IS risk incidents occur in context and differ one from another, incrementalist approaches to ISRM apply. This paper qualitatively draws viewpoints from IS management on the functionalist and incrementalist viewpoint of managing IS risk. We examine improvisation as an expression of extemporaneous action using a selected case study and argue that improvisation is a fusion of functionalist and incrementalist approaches. Discussions with information security practitioners selected from the case study suggest the presence of improvisation as a positive value-add phenomenon in ISRM. This paper presents a case for improvisation in ISRM.

Keywords: Improvisation, Information Security, Risk Management Functionalism, Incrementalism

1. Introduction

Business reliance on integrated computing globally has brought about many information security concerns. There has been a need to ensure confidentiality, integrity and availability of information in global integrated computing systems. This need has driven business and particularly information security practitioners to rely on various normative theories as frameworks that can help create stable environments (Siponen and Iivari 2006). Information Security Risk Management (ISRM), applies these normative theories within business contexts to ensure that technical and soft solutions exist for securing organizations' systems (Dhillon and Backhouse 2001; Siponen and Iivari 2006). Normative theories within ISRM usually have two main practical functions, namely a) to evaluate human/practitioners' action and b) to guide people's/practitioners' behaviour (Siponen and Iivari 2006). These two are based on normative logic that suggests action as either good or bad. In the present world of unpredictability in information systems security, judging action as good or bad based on kernel normative theories has proved difficult.

Anecdotes from information security practitioners suggest that during times of heightened uncertainty and exceptional situations, normative logic, (stemming from normative theories focused on imposing control and order) is usually followed. There has not yet been conclusive research which suggests that these control and order measures are sufficient. Emphasis of discussion on this paper is the 'exceptional situations' (Siponen and Iivari 2006) that give rise to the inconsistent application of normative theories in information security by practitioners in the course of their work. Exceptional situations have been recognized in Information Systems (IS) security literature (Baskerville1995; Dhillon and Backhouse 2001). While current research does not explicitly address or illustrate how these exceptional situations are handled in ISRM (Siponen and Iivari 2006), this paper recognises and promotes ***improvisation*** as a distinct way of handling exceptional situations.

The following sections discuss approaches in ISRM by practitioners: Section 2 discusses general issues in ISRM in brief. Section 3 discusses improvisation and the philosophy underlying these approaches. Section 4 contextualises research undertaken to examine these alternative approaches. This section also explains the research methodology. Section 5 discusses the research findings while section 6 gives a conclusion.

2. Information Security Risk Management

Historically, ISRM activities have been conducted in order to establish controls and security over information systems (Choobineh, *et al*. 2007). ISRM has therefore been a consistent way of strengthening security controls and practices at the organization level through risk analysis and continual improvement. The ISRM process has mechanisms in place designed to facilitate information security risk mitigation (Wiander and Holappa 2006) and is driven by organizational objectives. Baskerville (2005) has described two problems faced by information security practitioners, which limit the effectiveness of risk analysis practices. These include the lack of reliable empirical data concerning the frequency and amount of losses attributable to information security compromises, and the relative rarity of many kinds of information security compromises. Researchers have tried to examine information security risk in terms of the common challenges faced by information security practitioners in approaching and executing the ISRM process (Baskerville and Portougal 2003). Conventional methods of examining information security risk proposed by these studies include checklists, risk analysis and evaluation (Baskerville 1993; Birch and McEvoy 1992; Dhillon and Backhouse, 2001). The limitations of these techniques have been exacerbated by not including the socio-organisational aspects of information security, which researchers have found to be an important element in the development of an information security strategy (Backhouse and Dhillon 1996; Dhillon and Backhouse 2001).

3. The Improvisation Effect In Information Security

Researchers such as Bjo¨rck (2004) realized the need to look at ISRM in organizations afresh by postulating a neo-institutional theory in studying IT security issues in organizations. Bjo¨rck (2004) argues that the revolutionized modern organization requires new ways of explaining why formal security structures (***functionalism***) and actual security behavior (***incrementalism***) differ and why organizations often create formal security structures *without implementing them fully*. Such observations have lead us to have a closer look at organizational *improvisation* as a potentially relevant phenomenon for ISRM in current competitive environments (Crossan & Sorrenti 1997; Moorman & Miner 1998). Improvisation occurs in various forms as either individual improvisation or collective improvisation. ***Individual Improvisation*** is where planned or deliberate individual behaviour creates *improvisation* (Moorman and Miner 1998). As an illustration, an individual's deliberate behaviour may play an important role in speeding the development of highly iterative and experiential new products (Moorman and Miner 1998; Eisenhardt and Tabrizi 1995). ***Collective Improvisation*** is the combined effort of several individuals/organizations (Cunha 2004). Research suggests that interactions among people who are improvising frequently produce collective *improvisation* (Cunha 2004; Crossan and Sorrenti 1997). There are suggestions that collective *improvisation* often builds on and incorporates individual *improvisation* (Moorman and Miner 1998).

Ciborra *et al*. (2000) considered *improvised* activities as **simultaneously structured** (functionalist) and **unpredictable**; planned but emergent; discernible after the fact but spontaneous (incrementalism) in manifestation. *Improvisation* in organisations has been a phenomenon researched by social scientists due to its perceived importance in contextually relating content and sequence of previous processes and routines in novel ways that affect outcomes (Cunha 2004). The perspective illustrated in **Figure 1** below shows *improvisation* **as a fusion** between functionalism and incremental approaches to ISRM (Njenga 2007).

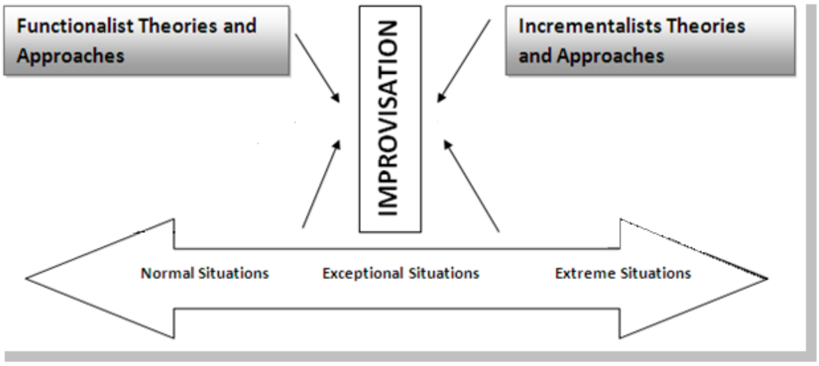
Functionalist Theories and Approaches
IMPROVISATION
Incrementalists Theories and Approaches
Normal Situations
Exceptional Situations
Extreme Situations

Figure 1. *The holistic view of Improvisation in ISRM (Adopted from Njenga 2007)*

Figure 1 provides a framework for conceptual thinking regarding IS security related improvisation that is guided by suggested kernel theories (i.e. both functionalist and incrementalist). IS security related improvisation manifests in two ways; First improvisation can result from short-comings or "functional gaps" in existing information systems. This primarily occurs in unanticipated (exceptional) situations and is often referred to as "*workarounds*" (McGann and Lyytinen 2008). Secondly, improvisations can result from an actor seizing new opportunities to configure existing IS capabilities into new functionality - referred to as "*configurable IT improvisations"* (McGann and Lyytinen 2008). Improvisation occurs in a continuum from normal to extreme situations and can arise from events for which no applicable rule (functionalist) exists (Saastamoinen 1995). Weick (1998) views the attributes of improvisation as a continuum ranging from taking minor liberties and adding "accents" to systems known as "***interpretation***"; through anticipating, rephrasing, regrouping, and adding clusters not originally included - known as "***embellishment***". This latter aspect results in full-scale "improvisation" meaning that there is transformation that results in the revised system having little resemblance to the original system (Weick 1998).

The framework discussed in **Figure 1** offers a baseline for a comprehensive analysis of improvisation in ISRM. It integrates functionalist kernel normative theories and incrementalist perspectives (planned, reflexive). Such phenomena are also referred to as being rational adaptive (Segars & Grover, 1999).. Having this framework in mind, the next section illustrates its application in an organisational setting through an in-depth case study. In this case study, we explored how information security practitioners handled exceptional situations within contexts of information security. The analysis illustrates improvisation in ISRM. Empirical data is deployed to illustrate interplay and fusion between kernel normative functionalist and incrementalist approaches to ISRM.

4. Research Methodology

4.1 Research Approach

The research combined theory building (Glaser and Strauss 1967) and a single case study (Yin 1994). The single case study research was exploratory, interpretivist and contextual. The case study approach was used because the study involved the examination of a complex social phenomenon. The selected case was also uniquely ***positioned*** to generate a full variety of evidence including documents, artefacts, interviews and observations. The benefit of interpretivism was that the researcher could retain "holistic and meaningful characteristics of real-life events" occurring within the context of information security in this organisation. The research method models Eisenhardt's (1989) approach and involved both theory generating and validating of conceptual elements.

Units of Analysis; the following units of analysis from the case were examined. 1. Information Assets Access and Data Control; 2. Information Security Architecture; 3. Information Security Policies; 4. Information Security Event Monitoring; 5. IT Governance and Regulatory Compliance; 6. Disaster Recovery and Business Continuity. The case organisation followed set procedures as directed by the CobiT, ITIL, ISO IEC 17799 frameworks and methodologies. It was therefore easy to map out the abovementioned units of analysis as activities defined by kernel theories.

4.2 Data collection

The primary data consisted of a series of 11 in-depth interviews. All interviews were tape recorded. After each interview, the information was transcribed verbatim in writing. In addition, notes were taken as the interviews progressed. It is from the transcribed responses from the interviewees that the research formed the contextual case for the phenomenon of *improvisation* being investigated. The interviews were conducted for 60 to 90 minutes per session. This generated close to 700 transcript minutes for data analysis.

4.3 The Use of Grounded Theory Techniques

The researcher used the grounded theory technique of open coding to inductively derive concepts of improvisation from empirical data (Glaser & Strauss 1967; Strauss & Corbin 1990; Glaser 1992) . Grounded theory techniques have been used successfully in both organizational and information systems research in the past

(Orlikowski 1993; Trauth & Jessup 2000). An explanation of each step of the research procedure is shown in **Table 2.**

Table 2. *Open Coding of Improvisational Date Incidents*

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos**	**STEP 4** **Level (Strategic, Tactical, or Operational)**	**STEP 5** **Concepts generated**
Extracting Data Incident; The researcher started by looking for elements of *improvisation*. The process of breaking down and analysing the data and assigning labels is described as content analysis by researchers (Glaser and Strauss 1967).	**Determining Context of Data Incident;** Through conversation analysis (Denzin et al. 2003) the researcher provided the context for selected data in the data-sets for incidents that reasonably suggested *improvisations*.	**Deriving Open Codes from Researcher's Memos;** The process of writing memos that would guide open coding (grounded theory technique) in STEP 3 involved several sub-steps. The first step was to examine in-vivo codes.	**Determining Level;** The inductive aspect of analysing data was made possible by extracting and understanding data that reflected aptitude for a fusion of structure and creative thinking simultaneously at three organisational levels.	**Creation of Codes and High Level Concepts Inductively;** Deriving codes was by way of examining data-sets in-depth and careful analyzing these.

5. Discussions and Analysis

The table above shows the methods used to extract instances of *improvisation* through discussions held with the information security practitioners. The next section is a more detailed discussion of *improvisation* as analysed by the researcher.

5.1 Functionalism and Incrementalism - Improvisation

New ways of thinking in ISRM was evident particularly in how practitioners managed information access and data control. Although there are specified procedures (functionalist) contained both in **ISO IEC 17799, Section 5.1** (prescribing how information security practitioners should treat information assets) and **Section 5.2** (prescribing acceptable ways for information control and classification), extemporaneous thinking regarding these procedures was revealed through discussions with practitioners. Discussions with Information Security practitioners firstly acknowledged the need to adhere to procedure, evidenced as follows;

> *"…and without preparation, [we needed] getting to know whether there is compliance, considering, information security you know whether there are best solutions to match the technology platform… stuff like that…"*

> *"Roles [end users roles] are specifically split into two areas, technical response and the process, procedures and people element"*

There were times when the practitioners would be forced to address information security control and access issues in an *out-of-the-box*, *spur-of-the-moment* fashion. In one particular instance, it was noted that access to sensitive information to a user who requested such access was granted spontaneously:

> *"…so we quickly had to make [create] a few more categories…so it doesn't just get as simple as you just having internet access and you didn't get this..."*

This act of spontaneity in determining access levels was a demonstration of the need to quickly address information access needs. The researcher proceeded to code this instance as **quick reaction.** At the heart of this kind of *improvisation* was the ability for the practitioner to react quickly and ingeniously, to overcome emergent and presented constraints. While there are specified compliance requirements for information architecture specifications, the **ISO IEC 17799 Section 12.1.1** explains the management obligation to design, operate and use information systems in ways that meet and address requirements stipulated by statutes, regulatory and contractual frameworks. The **CobiT** objectives **Section AI5.13** similarly suggests a manner for evaluation and meeting user requirements through post-implementation review to assess whether user needs are being met. **ITIL Section 3.5.4** (*ICT Infrastructure Management*) gives direction on system deployment and acceptance testing. Information security practitioners were aware of these requirements and had put in place procedures necessary for compliance. The organisation's architecture form was primarily responsible for this as shown by an extract of this data incident.

> *"…We have got the Architecture forum, which sits under [name withheld]… and uum, we also have [another forum], which I'm more involved in, in making sure that there is compliance architecture…*

Most of these procedures are incorporated in the overall information architecture specifications. In as much as these procedures were known to the practitioners, when faced with the challenge of identifying compliance requirements at the time, the information security practitioners showed unique ability to match compliance needs with pragmatic solutions. One information security practitioner was of the opinion that some of these compliance requirements in as much as they were important, had inherent gaps. These gaps left practitioners with little choice but to draw on their past experiences and any other cognitive or physical resource available in order to address the gaps and face IT challenges as they arose. In their words, "*they did what they had to do*" This was explained by one practitioner as follows:

> *"…I think our main thing here is to keep [going]… I mean we have a lot of good uses in policies when it comes to keeping the system going, certain time we do what we have to do to keep the [systems] going…and sometimes we don't…know if it is the right thing to do…"*

The context of the data incident was that when faced with challenges, there were no clear guidelines to follow hence "*sometimes we don't…know if it is the right thing to do*". While following procedure would mean following what was set, improvisation would have meant looking at procedure but re-creating new routines. This is what was done. In this case the practitioner showed that they acted outside of formal procedures. This was coded as being **rational adaptive.**

In all, 25 similar types of high level concepts (e.g., **quick reaction**, **rational adaptive**) specific to improvisation (either as individual or collective) were developed by the researcher through discussions with the information security practitioners. An important point about improvisation derived from these codes was that the phenomenon was demonstrated to be actively present at both individual and group (collective) level. If the improvisation was coded as being at the individual level, this simply meant that key information security practitioners were at an individual level altering their roles to meet the heightened demands of the emergency. Collective improvisation manifested itself as a combined effort of several information security practitioners whose aim was to create and enact novel scenes or situations simultaneously to solve problems that presented them. This can be explained as follows. During discussions the researcher could not help but notice the continued use of the word "*we*" for instance,

> *“…maybe we should actually do this in a different way… “*

> *“…I mean…a lot of it is in based on experience, and just knowing what is important and what’s not, we sit…and we put together our plan…”*

The context of the data incident was that during emergencies, there were no clear guidelines to follow and practitioners relied on experience. While following procedure would mean following what was set, *improvisation* would mean looking at procedure but re-creating new routines based on experience. Although collectively the group did not anticipate challenges or problem areas, they seemed to collectively work together to simultaneously coordinate solutions. There was a lot more of this collective coordination between practitioners as opposed to practitioners acting alone. Table 3 shows that the conceptual density of collective improvisation (19 instances) was much greater than individual improvisation (6 instances) for this specific case. These specific instances, (with example quotes), are also shown in Table 3.

Table 3. *Conceptual Density of Individual and Collective Improvisation*

Units of Analysis	**Concepts and Conceptual Density**			
Activities related to:	**Collective Improvisation**	**Individual Improvisation**	**Example (transcripts)**	**Count**
1 Information Assets Access and Data Control	*Manipulating*$^{\text{IMPROV-1}}$ *Quick reaction*$^{\text{IMPROV-2}}$ *Being deliberative*$^{\text{IMPROV-3}}$,		*“…and we did and worked on exactly what they said.. and of course within the first few days.. of putting access controls in [the system]…we got hundreds and hundreds of calls…saying they couldn’t get through.. they said that they wanted to go to selling sites.. whatever…and they couldn’t go to see what was on hundreds of other sites…”*	3
2 Information Security Architecture	*Novel*$^{\text{IMPROV-4}}$, *Rational adaptive*$^{\text{IMPROV-5}}$ *Deliberative*$^{\text{IMPROV-6}}$		*“and whether there is compliance, you know considering security you know whether there are best solutions to match the technology platform… stuff like that”*	3
3 Information Security Policies	*Rational adaptive*$^{\text{IMPROV-7}}$	*Lateral thinking*$^{\text{IMPROV-8}}$	*“ what they did was… they took the notebooks…they gave those new notebooks to people…and they gave the old notebooks[against policy due to expired warranties] that people had that were still on working conditions to other people “*	2

Units of Analysis **Activities related to:**	**Concepts and Conceptual Density**			
	Collective Improvisation	**Individual Improvisation**	**Example (transcripts)**	**Count**
4 **Information Security Event Monitoring**	*Being practical*$^{\text{IMPROV-9}}$ *Being ingenuous*$^{\text{IMPROV-10}}$	*Being creative*$^{\text{IMPROV-11}}$ *Rational adaptive*$^{\text{IMPROV-12}}$	*"well… what you see… well what happens is that it is all about saving money "* *"so there are those little things…that we do just to help us and to help the business.. because it's those quick little things that…we need to do better "*	4
5 **IT Governance and Regulatory Compliance**	*Being inspired*$^{\text{IMPROV-13}}$ *Rational adaptive*$^{\text{IMPROV-14}}$ *Creativeness*$^{\text{IMPROV-15}}$ *Resourceful*$^{\text{IMPROV-16}}$ *Getting by*$^{\text{IMPROV-17}}$ *Managing* $^{\text{IMPROV-18}}$	*Being novel*$^{\text{IMPROV-19}}$	*"yes but …like I said…had we not adopted CobiT at the board level, we would have made it far more difficult [to implement], but … and the challenge being the audit report"*	7
6. Disaster Recovery and Business Continuity	*Being-quick-witted*$^{\text{IMPROV-20}}$ *Lateral thinking*$^{\text{IMPROV-21}}$ *Rational adaptive*$^{\text{IMPROV-22}}$ *Managing*$^{\text{IMPROV-23}}$	*Being-quick-witted*$^{\text{IMPROV-24}}$ *Getting-by*$^{\text{IMPROV-25}}$	*" in order to give to the people [resources] that they gave…they got the ones that [were] broken…[and modified these] they had to think quick...and make that kind of a judgment…"*	6
Total Conceptual Instances of improvisation	***19***	***6***		***25***

5.2 Implications for Practice

The need to encourage improvisation would be justified since improvisation offers information security practitioners and practices various ways to remain flexible and adaptive in turbulent situations while allowing for co-presence efficiency and effectiveness in detecting change and immediately taking advantage of this change. It can be seen that the sets of improvisation (collective or individual) presented in this paper were essential and proved effective in ISRM processes. In general terms, however, improvisation proves only effective provided the information security practitioners are skilled enough and are capable of utilising the best available resources within a firm to achieve the intended purpose.

6. CONCLUSION

A concluding suggestion is that so long as practice is endowed with practitioners who are capable of skillfully manifesting improvised acts, whether individually or collectively, these acts should not be stifled, but made to flourish since they have been shown to be of value to ISRM. Practice should establish mechanisms to cope with the fear that various improvisations will override long nurtured functionalist structures. Improvisation will actually give contextual meaning to these very functionalist structures. For improvisation to be beneficial to ISRM, information security practitioners should perceive its intrinsic and extrinsic value. It is hoped that this discussion has highlighted this. Information security practitioners should see themselves as socio-constructive agents who are creative and who create reality around themselves. They should see improvisation as leading to a rich and good ISRM practice**.**

References

1. Backhouse, J. and Dhillon, G. "Structures of responsibility and security of information systems", *European Journal of Information Systems* Vol. 5:1 pp. 2-9. (1996)
2. Baskerville, R. "Semantic Database Prototypes," *Journal of Information Systems*, Vol. 3:2, pp. 119-144. (1993)
3. Baskerville, R. The Second-Order Security Dilemma. In W. Orlikowski, G. Walsham, M. Jones and J. DeGross (Eds.) Information Technology and Changes in Organizational Work. London: Chapman & Hall, pp. 239-249. (1995)
4. Baskerville, R. "Information Warfare: a comparative framework for Business Information Security", *Journal of Information System Security*, Vol. 1:1 pp. 23-50 (2005)
5. Baskerville, R., and V. Portougal. "A Possibility Theory Framework for Security Evaluation in National Infrastructure Protection," *Journal of Database Management*, Vol. 14:2 pp.1-13. (2003)
6. Birch, G.D.W. and McEvoy, N.A. "Risk analysis for information systems", *Journal of Information Technology*, Vol. 7, pp. 44-53. (1992)
7. Björck, F. "Institutional Theory: A New Perspective for Research into IS/IT Security". In *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37 2004),* 5-8 January, Big Island, HI, USA: IEEE Computer Society. (2004)
8. Choobineh, J., Dhillon, G., Grimaila, M.,R. "Management Of Information Security: Challenges And Research Directions" *Communications of the Association for Information Systems* Vol. 14:3 pp. 958-971 (2007)
9. Ciborra, C.; Braa K.; Cordella A.; Dahlbom b.; Hanseth O.; Hepso V.; Ljungberg J.; Monterio E.; and Simon K. A. '*From Control to Drift'*., Oxford University Press, Oxford: (2000)

10. Crossan, M M., and Sorrenti M., “Making Sense of Improvisation” *Advances in Strategic Management* Vol. 14 pp. 155-180 (1997)
11. Cunha, M., P. “Management Improvisation” *FEUNL Working Paper No. 460.* Available at SSRN: http://ssrn.com/abstract=882455 (2004)
12. Dhillon, G. and Backhouse, J. “Current Directions in IS Security Research: Toward Socio-organizational Perspectives,” *Information Systems Journal* Vol. 11: 2. (2001)
13. Eisenhardt, K.M. "Building Theories from Case Study Research," *Academy of Management Review* Vol. 14:4 pp. 532-550 (1989)
14. Eisenhardt, K.,M. and Tabrizi B., N. "Accelerating Adaptive Processes: Product Innovation in the Global Computer Industry " *Administrative Science Quarterly*, Vol. 40:1 pp. 84-110 (1995)
15. Glaser, B.G. “*Basics of Grounded Theory Analysis: Emergence Vs. Forcing*”. Sociology Press: California. (1992)
16. Glaser, B.G. & Strauss, A. L. “*The Discovery of Grounded Theory: Strategies for Qualitative Research*”. Aldine Transaction: New Jersey. (1967)
17. McGann, S.T., and Lyytinen, K., “The Improvisation Effect: A Case Study of User Improvisation and Its Effects on Information System Evolution”, *Proceedings of the 29th International Conference on Information Systems (ICIS),* Paris, France *(*2008)
18. Moorman, C., and Miner, A. “Organisational Improvisation and Organisational Memory,” *Academy of Management Review* Vol. 23:4 pp. 698-723 (1998)
19. Njenga, K., “Conceptualising Improvisation in Information Security Risk Management Activities”, *(Doctoral Consortium) Proceedings of the 11th Pacific Asia Conference on Information* Auckland, New Zealand (2007)
20. Orlikowski, W.J. “CASE tools as organizational change: investigating incremental and radical changes in systems development”, *MIS Quarterly,* Vol. 17:3 pp. 309-40. (1993)
21. Saastamoinen, H. “On the handling of exceptions in information systems”. *Computer Science, Economics and Statistics”* Jvaskyla, University of Jvaskyla: 195 (1995)
22. Segars, A. & Grover, V. Profiles of strategic information systems planning. *Information Systems Research*, 10(3): 199-232 (1999)
23. Siponen, M., and Iivari, J., Six Design Theories for IS Security Policies and Guidelines, Journal of the Association for Information Systems Vol 7:7 pp 445-472 (2006)
24. Strauss, A., and Corbin, J. “*Basics of qualitative research: Grounded theory procedures and techniques*”. Sage Publications, Newbury Park, CA (1990)
25. Trauth, E. M. and Jessup, L. M. “Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use”, *MIS Quarterly,* Vol. 24:1 pp. 43-79. (2000)
26. Weick, K. ‘Improvisation as a mindset for organizational analysis’, *Organization Science*, Vol. 9:5 pp. 543–555 (1998)
27. Wiander, T., and Jarkko M. Holappa, J., M. “Theoretical framework of ISO 17799 compliant information security management system using novel ASD method”. proceedings of the *IAEA Technical Meeting on Cyber Security of Nuclear Power Plant Instrumentation, Control and Information Systems”,* 17-20, Idaho Falls, USA (2006)
28. Yin, R., K. “*Case Study Research, Design and Methods”, (*2nd ed.) Sage Publications, Newbury Park, CA (1994)