INDUCTIVELY DERIVING AN ORGANISATIONAL INFORMATION SECURITY RISK MANAGEMENT AGENDA BY EXPLORING PROCESS IMPROVISATION

[*1] Kennedy N Njenga

[*2] Irwin Brown

[*1] Department of Business IT, University of Johannesburg; Tel: 011 559 1253

[*2] Department of Information Systems, University of Cape Town: Tel: 021 650 2677

ABSTRACT

In times of heightened uncertainty and unpredictability it is believed that incrementalist approaches that are not resolute to order and control in information security risk management (ISRM) are necessary. This is because information security incidents that occur in context are noted to differ one from another. Incrementalist approaches to ISRM apply when contextual security risk instances are rare, unique and complex. This paper qualitatively explores and draws viewpoints from information security management on the incrementalist viewpoint of managing information security risk. Attention is given to *process improvisation,* an explication of combined functionalism and incrementalism which places an emphasis on ways in which practitioners creatively mitigate information security risk. An in-depth case study approach has been used to explore this phenomenon and grounded theory techniques employed to analyse the data. The process of inductive theory building that serves as impetus for an ISRM agenda shows the fit between data and the emerging theory on process improvisation. Findings highlighted in this paper yield rich insights about how an ISRM agenda may incorporate incrementalist and functionalist approaches. Implications for such an agenda to practising information security professionals are also presented.

KEY WORDS

Information Security, Risk, Process Improvisation, Incrementalism, Agenda-setting

INDUCTIVELY DERIVING AN ORGANISATIONAL INFORMATION SECURITY RISK MANAGEMENT AGENDA BY EXPLORING PROCESS IMPROVISATION

1 INTRODUCTION

Information Security Risk Management (ISRM) professionals take an approach to security that is often guided by; importance of security, user perception, costs, availability and compliance with laws rules and regulations (Jochem *et al.* 2006). These approaches according to Dhillon & Backhouse (2001) are functionalist and are the *oppositus* of incrementalism. Functionalist approaches are those approaches that are resolute to order and are evidenced by numerous publications that offer normative guidelines for design, implementing and managing secure information systems (Baskerville 1988; Straub & Welke 1998). Functionalist frameworks for information security that for instance use CobiT or Code of Practice for Security Management have evolved from an inventory of resources and threats from which risk profiles are created (Jochem *et al.* 2006). Hu *et. al.* (2007) has outlined functionalism in information security by considering how modern organisations have established routines and order to cope with internal and external influences of information security risk.

In times of heightened uncertainty and unpredictability it is believed that incrementalist approaches that are not resolute to order and control in information security risk management (ISRM) are necessary. This is because emergent technology, increased usage of computers and the internet has created risks and along with this much uncertainty (Siponen and Kukkonen 2007). Incrementalist approaches to ISRM apply when contextual security risk instances are rare, unique and complex. It is expected that approaches that are incremental can mitigate risk and lead to normalisation of situations.

This paper holds the view that agenda-setting for ISRM takes cognisance of functionalist approaches to ISRM to the detriment of incrementalism. Setting the agenda for ISRM has therefore been largely influenced by the choices in functionalism postulating salience transfer in

ISRM. Salience transfer is the ability to transfer issues perceived important into corporate ISRM agendas. Corporate agenda in ISRM are issues that big business and corporations consider important.

The purpose of this research was to conceptualise how salience transfer in ISRM agenda-setting could be made richer by understanding the combination of incrementalist and functionalist approaches as impetus to ISRM agenda-setting. This research explored *improvisation* and specifically how *process improvisation*, as an explication of both incrementalism and functionalism was manifested in ISRM activities and its possible influence to corporate ISRM agenda. The research makes a theoretical contribution by arguing that agenda-setting in ISRM may also take cognisance of combined incrementalist and functionalist approaches.

The paper is structured into five main sections. This first section has introduced and set the context for research. In the next section the various approaches to ISRM are discussed. In this section, functionalism and incrementalism in ISRM are examined in detail. *Process improvisation* in organizations as an explication of both incrementalism and functionalism is also discussed in this section. What follows is a description of agenda setting in ISRM. The third section is the description of the research and justifies the use of a single case study. The research methodology applied is also discussed. In this section also, the use of grounded theory techniques is explained and justified. The fourth section presents and discusses the research findings which are subsequently used to construct a model for agenda-setting in ISRM. By use of the constructed model, this section discusses the possible influence of *process improvisation* to ISRM agenda. In the fifth section concludes the paper by explaining possible benefits of *process improvisation* for information security practitioners.

1.1 Research Value

Little research has been undertaken, to explain salience transfer of combined incrementalist and functionalist approaches to ISRM agenda-setting. This research aims at providing deeper insights into this discussion.

2 APPROACHES TO ISRM

Organisations currently manage ISRM by focussing on planning and implementing procedures and guidelines as contained in a standard code

of practise such as ISO 17799 (Eloff & Eloff 2003; ISO 17799). Dhillon (1997), Dhillon & Backhouse (2001) and Hirschheim *et. al.* (1989) have analyzed existing ISRM methods in the light of formalized rule structures in designing and managing security. An information security planning methodology has also been suggested by Straub & Welke (1998).

2.1 Functionalist and Incrementalist Approaches to Information Security Risk Management

Researchers in information security who have suggested, rational choice (Wheeler and Venter 2006) and clear structured policies as being one of the ways to deal with risks and uncertainties are, for the purpose of this research, classified as **functionalist approaches (**Von Solms and Von Solms 2005; Vorster and Labuschagne 2006)**.** Von Solms (2006), talks of structured frameworks for internal controls and policies that are directed and managed by organizations. There are also researchers have become aware of an increasing number of 'new' approaches that explore alternative perspectives related to the interpretive, radical humanist and radical structuralist paradigms. These latter paradigms are based on sociological and philosophical theories (Hu *et al.* 2007). Researchers using these latter approaches which call for alternative ways of understanding ISRM have been classified as **incrementalists**. Salmela *et al*. (2000) highlighted principles of the incremental approach, when observing a particular organization's activities. They described the incremental approach as **highly reflexive**, with decisions being made at any time. The way in which the incremental approach in organizations was observed can also be compared with theories related to reflexivity such as **contingency theory**. Adler *et al.* (1999) exemplified contingency theory when making reference to efficient organisations which were designed to fit the nature of their primary tasks. It should be noted that some organisations practise the incremental approach whereby functionalism takes a small part while activities and decision making are made on a one-by-one basis.

2.2 Process Improvisation: Combined Functionalism and Incrementalism

Formulation of information security policies that take cognisance of both functionalism and incrementalism i.e. information security risk management, and strategic information systems plan (SISP) has been proposed by Doherty (2006) as a way adding richness to both disciplines. Similarly, researchers such as Bjo¨rck (2004) realized the need to look at 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. It has been from such observations that has lead researchers to have a closer look at have organizational *improvisation* by showing its relevance in current competitive environments (Crossan & Sorrenti 1997; Moorman & 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 its manifestation. *Process improvisation* as a type of 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 2003). *Process improvisations* affect the manner in which products are developed Miner *et al.* (2001).

2.3 Agenda-setting in ISRM

It can be noted that first-level agenda setting as traditionally studied by researchers use objects or issues to influence the people. The formation of an ISRM agenda depends on information security practitioner conception of what is important in ISRM. It has been noted that information security practitioners often set an ISRM agenda that is devoid of incrementalism. This is because incrementalism has not been counted as important because of its "soft" appeal i.e. a derivative from the social sciences. Understanding *process improvisation* (as a fusion approach) in ISRM could help reconcile tension between structure (functionalism) and

reflexivity (incrementalism) and set the pace for a richer agenda-setting since it comprises a rich mixture of centralised structure and novel spontaneity (Cunha 2004; Ciborra *et al.* 2000; Segars and Grover 1999). In this way information security practitioners may be forced to think about such issues and therefore involves salience transfer among practitioners.

3 METHODOLOGY

A single case research was used which was exploratory, interpretivist and contextual. The researcher identified and selected a single case on the assertion that this case was ***uniquely positioned*** to generate a full variety of evidence including documents, artefacts, interviews and observations.

3.1 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.

3.2 Units of Analysis in the Single Case

The single case followed set procedures as directed by the CobiT, ITIL, ISO IEC 17799 frameworks and methodologies. It was therefore easy to map out the units of analysis as activities defined by these frameworks, since these activities ***were already implemented*** in the organisation. There was a clear structure of how these activities were to be implemented and performed (based on CobiT, ITIL, ISO IEC 17799)**.** The ISRM activities and hence the units of analysis are summarised in **Table 1** below.

Table 1. Open Coding of Improvisational Date Incidents

Units of Analysis	**ISO IEC 17799**	**ITIL**	**CobiT**
Information Assets Access and Data Control	***Section 3 of ISO 17799***	**Application Management, Control Methods and Techniques** 7.2 Understanding the applications relationship to IT services	**DS 11** Manage Data
Information Security Architecture	***Section 4 of ISO 17799***	**ICT Infrastructure Management, Technical support** 5.4	**PO 2** Define the Information Architecture
Information Security Policies	***Section 5 of ISO 17799***	**Security Management;** *Fundamental of Information Security;* 4.1 Control	**DS 5** Ensure Systems Security
Information Security Event Monitoring	***Section 9 of ISO 17799***	**Service Level Management***;* 4.4.7 Establish monitoring capabilities	**DS 10** Manage Problems and Incidents
IT Governance and Regulatory Compliance	***Section 12 of ISO 17799***	**The Technical Support** 5.4 The technical support process	**PO 8** Ensure Compliance with External Requirements
Disaster Recovery and Business Continuity	***Section 12 of ISO 17799***	**Availability Management** 8.3 The availability management process	**DS 4** Ensure Continuous Service

3.3 Inductive Theory Building and the Use of Grounded Theory Techniques

Inductive theory building emphasizes the fit between data and the emerging theory, rather than moving deductively down from a prior hypothesis. The researcher used the grounded theory techniques of open coding to achieve this. Grounded Theory Techniques (GTT), (Glaser & Strauss 1967; Strauss & Corbin 1990; Glaser 1992) formed a basis for

content analysis (see ***step 1*** below). GTT also for purposes of this research proved an attractive way for inductive reasoning. Orlikowski (1993) and Trauth & Jessup (2000) have demonstrated successfully GTT application in organizational and information systems research in the past What follows is a detailed explanation for each step as shown by **Table 2.**

Table 2. Open Coding of Improvisational Date Incidents

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researc her's memos**	**STEP 4** **Level (Strategic, Tactical, or Operational)**	**STEP 5** **Concepts generated**
Extracting Data Incident; The researcher started by looking for elements of *process 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 *process 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.

4 RESEARCH FINDINGS

This section provides a summary of units of analysis from the single case and the data-sets examined in each unit of the case. In total, a series of **23 concepts** (high level concepts) were generated from open coding that were interpreted to be *process improvisational* actions in ISRM. There were more conceptual instances of concepts relating to *process improvisation* at Event Monitoring activities than other activities for this case. The case also suggests that improvisations were less likely to be present in activities relating to IT Governance and Regulatory Compliance. This is shown by *Figure 1* (next page). The case also suggests that process improvisation was much more presented at operational rather than at strategic levels within the organisation.

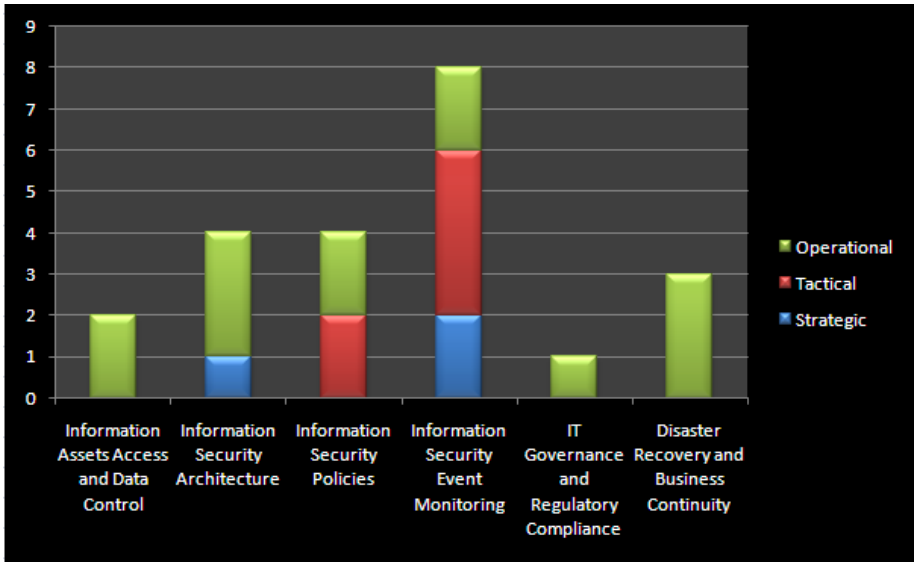

Figure 1. Process Improvisation in ISRM activities

4.1 Deriving an ISRM Agenda: Theoretical Synthesis

Research findings show that the occurrence of *process improvisation* was in many cases ***contextual*** due to security incidents being rare and unique. These incidents therefore required a novel way of handling these

particularly at activities relating to Event Monitoring. Only by hindsight would practitioners' perceive that they were *process improvising*.

Insights as to these revelations led the researcher to conceptualise on how an ISRM agenda would be formulated, which brought awareness of these to ISRM practitioners. There would be different ways by which practitioners would perceive this information. They would as explained by Eriksson and Noreen (2002);

a) Realise the importance of *process improvisation* in ISRM and hence set the agenda; (*agenda-setting).*

b) Realise that *process improvisation* has not effect in ISRM, hence be removed; (*agenda removal*).

c) Realise that encouraging *process improvisation* would be interpreted as discouraging structure and functionalism and would therefore be deliberately be prevented from being discussed (*agenda blocking*)

d) Discuss the importance of process improvisation but this would not necessarily translate into concrete action of formalising it (*agenda structuring*). *Figure 2*. below summarises this discussion.

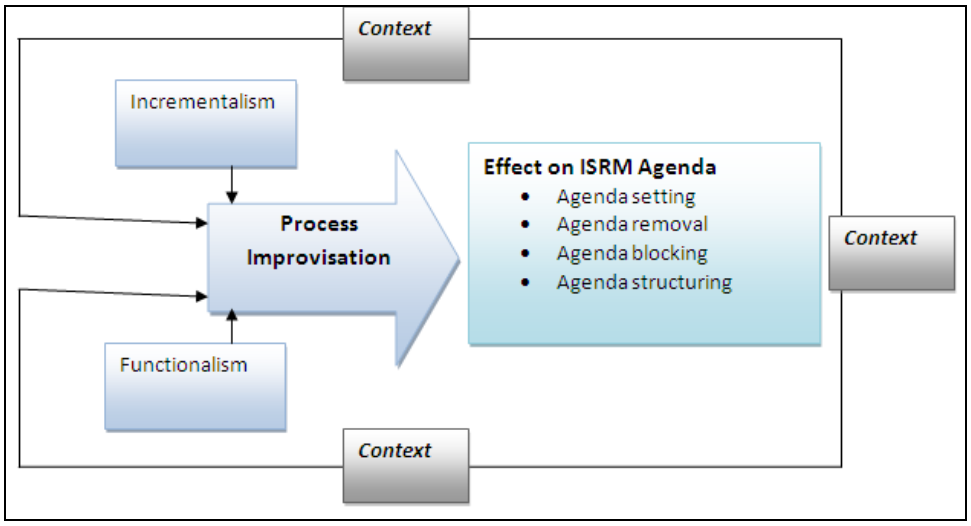

Figure 2. Inductively deriving an ISRM agenda: Adapted from Eriksson and Noreen (2002)

4.2 Implications for Practices

The researcher is of the opinion that it takes a discrete, bold, conscious step towards bridging this theory and practice. The need to encourage *process improvisation* would be justified since *process 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.

5 CONCLUSION

For *process improvisation* to be included as an agenda item in ISRM information security practitioners should perceive its importance. 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 ***process improvisation as leading to a rich and good ISRM practice.***

6 REFERENCES

Adler, P. S., Goldofta B. and Levine D. I., (1999) "Flexibility verses Efficiency? A case Study Model of Changeovers in the Toyota Production System" *Organization Science* Vol. 10:1 pp. 43-68

Baskerville, R., (1988) "*Designing Information Systems Security"* John Wiley & Sons, New York, NY.

Björck, F. (2004). "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 2004, Big Island, HI, USA: IEEE Computer Society.

Ciborra, C.; Braa K.; Cordella A.; Dahlbom b.; Hanseth O.; Hepso V.; Ljungberg J.; Monterio E.; and Simon K. A. (2000) '*From Control to Drift'*., Oxford University Press, Oxford:

Crossan, M. M., and Sorrenti, M., (1997) "Making sense of Improvisation" *Advances in Strategic Management,* Vol 14:0 pp. 155-180.

Cunha, M. P., (2003). "Organizational improvisation and change: two syntheses and a filled gap", *Journal of Organizational Change Management* Vol. 16:2 pp. 169-185.

Cunha, M., P. (2004) "Management Improvisation" *FEUNL Working Paper No. 460.* Available at SSRN: http://ssrn.com/abstract=882455

Deetz, S. (1996) "Describing Differences in Approaches to Organization Science: Rethinking Burrell and Morgan and their Legacy," *Organization Science* Vol. 7:2, pp. 191–207

Dhillon, G. (1997) "*Managing Information Systems Security",* MacMillan Press LTD. United Kingdom.

Dhillon, G. and Backhouse, J. (2001) "Current Directions in IS Security Research: Toward Socioorganizational Perspectives," *Information Systems Journal*, Vol. 11: 2.

Doherty, N. F. (2006) "Aligning the information security policy with the strategic information systems plan. *Computers & Security* Vol. 25:1 pp. 55-63

Eloff, J., and Eloff, M., 2003 "*Information Security Management – A New Paradigm"* Proceedings of SAICSIT 2003, pp. 130 –136.

Eriksson J., and Noreen, E. (2002) 'Setting the Agenda of Threats: An Explanatory Model', *Uppsala Peace Research Papers No. 6. Uppsala:* Department of Peace and Conflict Research, Uppsala University.

Glaser, B., G. and Strauss A (1967) "*The Discovery of Grounded Theory: Strategies for Qualitative Research"*, Aldine Publishing Co, Chicago IL.

Glaser, B.G. (1992). "*Basics of Grounded Theory Analysis: Emergence Vs. Forcing*". Sociology Press: California.

Hirschheim, R. and Klein HK, (1989) "Four Paradigms of Information Systems Development" *Communications of the ACM*, Vol 32:10, pp. 1199–1215.

Hu, Q., Hart, P., and Donna Cooke, D., (2007) "The role of external and internal influences on information systems security – a neo-institutional

perspective", *Journal of Strategic Information Systems* Vol 16:0 pp. 153–172.

ISO/IEC 17799 Code of practice for Information Security Management, International Organization for Standardization/ International Electrotechnical Commission. Available at http://www.iso.ch/iso/en/ISOOnline.openerpage

Jochem, A., Bewier, A., Bongers, L., Borger, L., Coene, H., Elsinga, B., Jonkman, E., Kuiper, R., Oostdijk, M., Rijsenbrij, D., Smulders, A. (2006) "Security Principles: Information security on the management agenda" *Genootschap van Informatie Beveiligers (GvIB) Expert Letter*, Volume 1:3 pp. 1-11

Miner A. S., Bassoff P. and Moorman C., (2001) "Organizational Improvisation and Learning: A Field Study" *Administrative Science Quarterly* Vol. 46:2 pp. 304-337

Moorman, C., and Miner, A. (1998) "Organisational Improvisation and Organisational Memory," *Academy of Management Review* Vol 23:4 pp. 698-723.

Orlikowski, W. J., (1993) "CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development" *MIS Quarterly* Vol 17:3.

Salmela, H., Lederer, A.,L. and Reponen, T. (2000) "Information systems planning in a turbulent environment" *European Journal of Information Systems* Vol. 9:1 pp. 3–15

Segars, A. & Grover, V. (1999) Profiles of strategic information systems planning. *Information Systems Research* Vol. 10:3 pp.199-232

Siponen, M. T., and Kukkonen, H. O., (2007) "Of Information Security Issues and Respective Research Contributions," *The DATA BASE for Advances in Information Systems* Vol 38:1.

Straub, D. and Welke, R. (1998) "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly* Vol 22:4 pp. 441–470.

Strauss, A. and Corbin, J. (1990), "*Basics of Qualitative Research: Grounded Theory Procedures and Techniques*" Sage, Thousand Oaks, CA.

Trauth, E.M. and Jessup, L.M. (2000) "Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use," *MIS Quarterly* Vol. 24:1 pp. 43-79.

Von Solms, B. (2006). "What every Vice-Chancellor and Council Members should know about the use of ICT" Proceedings of the Conference on Information Technology in Tertiary Education, Pretoria, South Africa.

Von Solms B and Von Solms R (2005) 'From Information security to…business security'? Computer and Security Vol 24:4 pp 271-273.

Vorster A., and Labuschagne L. (2006). "A new comparison framework for information security risk analysis methodologies", South African Computer Journal, Vol 37 pp. 98 – 106.

Wheeler M., and Venter H. (2006). " Change Management: A case study at the University of Pretoria", Proceedings of the Conference on Information Technology in Tertiary Education (CITTE) Pretoria, South Africa.