COLLECTIVE IMPROVISATION:

COMPLEMENTING INFORMATION SECURITY

FRAMEWORKS WITH SELF-POLICING

[1]Kennedy Njenga

[2]Irwin Brown

[1]Department of Business Information Technology, University of Johannesburg; Tel 011 559 1253 Email: knjenga@uj.ac.za

[2] Department of Information Systems, University of Cape Town; Tel 021 650 4260 Email: Irwin.Brown@uct.ac.za

ABSTRACT

The approach to information security governance has predominantly followed a functionalist paradigm with emphasis placed on formalized rule structures and policy frameworks. The alternative socio-organisational (reflexive) approach has in the recent past grown in prominence due to the emergent socio-organizational aspect of technologies and processes. This paper challenges the epistemology of the functionalist approaches which assumes predictability. Information security practitioners realize that much of their activities are adapted to fit emergent changes. The aim of this paper is to explore an antidote to functionalist structured approaches by conceptualizing collective improvisation and *self-policing*. A case study approach that incorporates grounded theory techniques is employed for this purpose. Tentative findings reveal that collective improvisation is most pronounced in activities related to operational activities in governance. The implications of these and other findings are also discussed.

KEY WORDS

Information Security Governance, Collective Improvisation, Self-Policing

COLLECTIVE IMPROVISATION:

COMPLEMENTING INFORMATION SECURITY

FRAMEWORKS WITH SELF-POLICING

1 INTRODUCTION

When the United States congress enacted the Sarbanes-Oxley Act of 2002 ("SOX") to protect investors and combat corporate crime, what followed was an active role by corporate directors and by extension, security practitioners who became mandated to improve corporate governance and information security governance. Von Solms & Von Solms (2004) have called for broader responsibilities by management regarding information security.

According to Von Solms (2006), corporate governance consists of structured frameworks for internal controls and policies that are directed and managed by organizations. Information security governance is seen as a subset of organizations' overall corporate governance program. Structured frameworks in information security governance include CoBIT, King, COSO, and ISO 17799 (explained further in the subsequent sections). The design of many of these frameworks can be explained by understanding the functionalist paradigm and approach which is evidenced by numerous publications that offer normative guidelines for implementing and managing secure information systems (Baskerville 1988; Straub & Welke 1998).

In recent times, Hu *et al.* (2007) has argued for a more coherent socio-organizational framework that explains deviation from a 'functionalist only' approach. They propose a holistic framework that takes into account practitioners' unique reflexive behaviour. Reflexivity refers to the reconfiguration of normative orientations that guide actors and organisations (Beck 1997). Ogus (2000) talks of reflexivity in terms of reforming the conventional structures of 'command and control' governance. This paper introduces an insightful alternative by proposing a multi-faceted approach that includes reflexivity and collective improvisation into the domain of

information security governance. Improvisation, derived from the Latin word '*improviso*' is defined as 'situated performance where thinking and action occur simultaneously and on the spur-of-the-moment' (Ciborra 1999). According to Ciborra (1999), collective improvisation refers to the combined improvisational effort of several individuals or organizations. The motivation for this research is of interest since the current thinking regarding information security governance is not well-known. Ciborra *et al.* (2000) has documented improvisation in organisations and explains it as a simultaneously structured and unpredictable, often emergent and opaque phenomenon. The nature of this paper extends an analytical understanding of collective improvisation in information security activities and proposes the following research question that contextualises the issue;

How is collective improvisation manifested in information security governance activities?

In addition, the paper aims at exploring how collective improvisation influences practitioner's actions towards understanding information security governance issues. The paper makes a theoretical contribution by arguing that practitioners' engagement with policy is essentially driven by novelty and reflexivity and expressed as *self-policing*. *Self-policing* is a concept that often leads to less enforcement activity and deterrence (Innes 1999).

The paper is structured into six main sections. This first section has introduced and set the context for research. In the second section the functionalist approach is introduced. The third section presents a multi faceted improvisational approach. The fourth section describes the research methodology. In this section, the use of grounded theory techniques is explained and justified. The fifth section presents and discusses research findings. In the final sixth section the paper is concluded by deriving implications for IS practitioners and researchers.

2 PREDICTIVE KNOWLEDGE: THE FUNCTIONALIST PARADIGM

Information security researchers have recognized the significance of well planned sound information security policies that focus on clear methodologies and programmes (Von Solms & Von Solms 2005; Schultz 2005). In their studies in Information Security, Dhillon & Backhouse (2001) have noted the dominance of the functionalist approach that emphasizes

formalized rule structures in designing and managing security. It is the notion of predictive knowledge that has influenced the functionalist approach to formulating policies for monitoring and control (Wheeler and Venter 2006). Predictive knowledge hence reinforces the functionalist paradigm when viewing designers and practitioners as solely technical experts (Wheeler and Venter 2006).

Predictive knowledge assumes the intent by users to follow order, maintain status quo and reinforce rational choice (Wheeler and Venter 2006). The functionalist structured approaches to information security have generated interest among information security researchers (e.g. Straub and Welke 1998; Siponen 2000; Von Solms and Von Solms 2005; Vorster and Labuschagne 2006) and is characterised by the use of many policies, frameworks and standards meant to foster order and control. **Figure 1-1** points to one of the many structured functionalist approaches to information security governance noted by the researcher.

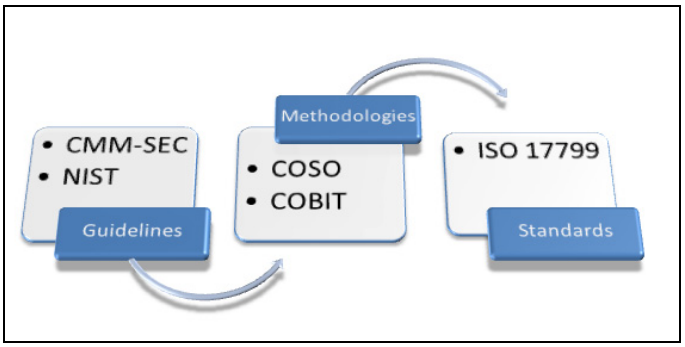

Figure 1-1 Structured Functionalist Approach to Information Security Governance

2.1 Guidelines

Information security governance is endowed with rich functionalist guidelines which provide direction for the activities or process to achieving set goals. The Capability Maturity Model for Security (CMM-SEC) is an example of a guideline that defines the process an enterprise must go through to move from limited security capabilities to increasingly optimizing protection postures (Burton Group 2005). The National Institute of Standards and Technologies (NIST) has issued guidelines under the

banner of the *Risk Management Guide for Information Technology Systems* in its Special Publication 800-30 (NIST SP 800-30). The ISO/IEC Guide 73 released jointly by the International Organization of Standards (ISO) and the International Electro-technical Commission (IEC) provides specific guidance on terms and definitions of concepts related to risk management.

2.2 Methodologies and Frameworks

There are a variety of functionalist methodologies in use to identify, measure, control and monitor information security risks. These stem either from government regulations e.g. Sarbanes-Oxley Act (SOX) or industry recommendations such as CoBIT™, COSO, (Committee of Sponsoring Organisations of the Treadway, Commission, (*Internal Control—Integrated Framework*, 1992). There is also Turnbull in the UK, CoCo in Canada, KING II, in South Africa and the IT Infrastructure Library (ITIL) for IT service management.

2.3 Standards

Standards are also functionalist in nature and are continually developed for the purpose of serving as measures for organizations to achieve desirable ends. They fall short of the main purpose of guidelines and frameworks since these do not show how to achieve stated ends. The latter assist organizations by showing how these stated ends may be achieved. An example of a prominent standard in use in South African is the ISO/IEC 17799 standard adopted from the British Standard BS 17799.

It is only by a closer examination of the information security risk management process and specifically the policy adoption process does one realize that information security activities are guided by an approach that is multi-faceted and not restricted to only blindly following frameworks, guidelines or standards in a purely functionalist manner.

3 REFLEXIVITY AND IMPROVISATION

Even as early as the 1970's scholars and researchers of systems thinking (Cleveland 1973) generated ideas of the need for holistic systems approaches to management. Cleveland (1973) argued on the need to match what became known as unsystematic reality with 'constructive ambiguity'. This argument opposed the functionalist premise while proposing that the management systems then, were too exact, too clear and therefore too rigid.

In the present times, the same attributes are still common in many organizations and have been instrumental in shaping and monitoring policy. The main problem with this thinking then and now is that in an effort to build efficient systems, scholars have been tempted to analyse and view everything systematically, while avoiding the soft socio-cognitive aspects of purposes and meaning. The gap in approach has been filled presently by studies relating to reflexivity and improvisation (Ciborra 1999; Ogus 2000). Much has been written concerning improvisation, strategy formulation and implementation (Perry 1991). These studies acknowledge actions that provide for reflexivity, in the sense that activities could be done in more that one way and each way finely fitting the situation (Scribner 1984). *Self Policing* is seen as the expression of reflexivity and increases efficiency in governance in two ways; one, remediation is achieved early; two, there is reduction in enforcement effort (Innes 1999). In an effort to understand this soft discourse, the next section presents the methodology that was used.

4 RESEARCH METHODOLOGY

A single case research strategy was employed, which was exploratory, interpretive and contextual. It sought to generate new insights into the phenomenon of collective improvisation in information security. As a pointer, this researcher drew a level of comfort from the interpretive paradigm. The researcher was able to identify, examine and evaluate the phenomenon of collective improvisation through the subjects' eyes and from the subjects' perspective (Hu *et. al*. 2007; Strauss & Corbin 1998). The interpretive paradigm permitted the researcher to provide useful insights that integrated the technical and the sociological human aspects of information security.

4.1 Grounded Theory Techniques

The researcher used grounded theory techniques to inductive derive a framework that emphasizes the fit between data and 'reality'. Grounded theory techniques, (Glaser & Strauss 1967; Glaser 1978; Strauss 1987; Strauss & Corbin 1990) formed a basis for content analysis of raw data and proved an attractive means for inductive reasoning. It should be noted that grounded theory has been used successfully in both organizational and information systems research (Orlikowski 1993; Sarker *et. al.* 2001; Trauth & Jessup 2000; Urquhart 1997).

4.2 Data Collection

Gathering primary data on information security proved to be challenging. What was experienced confirmed the findings of Kotulic & Clark (2004) namely that organisations are reluctant to share information about security policies with individuals from outside the company. The primary data was gathered and consisted of a series of 11 in-depth interviews with senior practitioners. The single organization was a large multi-national corporation.

5 RESULTS AND INTERPRETATION

The researcher used ISO 17799 domains to establish **Units of Analysis** or activities common in information security governance that employed a high degree of collective cognitive abilities. The researcher then interviewed practitioners engaged in these activities. The recorded interviews were transcribed and arranged into themes related to each of these units for analysis. Codes were derived from the transcripts that would help establish the level of conceptual density of instances of reflexivity and collective improvisation in these units. High level concepts were derived from these codes. What followed was the deriving of still even higher level categories from the concepts related to collective improvisation in each of the units. **Table 1** shows a mapping of the units of analysis to the ISO 17799 structured domains.

Table 1. Mapping ISO 17799 Domains to Research Units of Analysis

CORE InfoSecurity Management Activities ISO 17799 Sections			Re-search ed	Unit of Analysis
	Section	Type of Activity (Domain)		
	1	Introduction Reference text n/a	n/a	n/a
IDENTIFY	2	Introduction Reference text n/a	n/a	n/a
	3	Security policy	Yes	3 Information Security Policy
	4	Security organisation	*No	
	5	Information Asset Classification and Control	Yes	1 Assets control
ANALYSE	6	Personnel Security	*No	
	7	Physical and Environmental Security		2 Information Architecture Security
	8	Communications and Operations Management	*No	
RESPOND	9	Access Control	*No	
	10	System Development and Maintenance	Yes	4 Event Monitoring
	11	Business Continuity and Management	Yes	6 Business Continuity
	12	Compliance with legal requirements	Yes	5 Governance and Regulatory Compliance

* No – *activities that were deemed to lack any depth in cognitive- reflexivity were not researched on*

The understanding and integration of concepts and categories was done iteratively (Glaser & Strauss 1967). **Table 2** below shows the process

undertaken by the researcher to analyse data using grounded theory techniques.

Table 2. Research Process

RESEARCH PROCESS			
Process 1	**Analyse data relating to the** first unit of analysis to conceptualise improvisation	Use open coding	Develop concepts, and categories relating to improvisation in information security activities
Process 2	Theoretical sampling	Literal and theoretical replication across cases (go to process 3 until theoretical saturation)	Confirms, extends, and sharpens theoretical framework by analysing the rest of the units of analysis
Process 3	**Analyse data relating to** the subsequent other units of analysis to conceptualize improvisation	Use open coding	Develop concepts, and categories relating to improvisation in information security activities
Process 4	Explore relationships between concepts and	Use axial coding	Develop connections

RESEARCH PROCESS			
	Categories from all units of Analysis	Use selective coding	between a category and its sub-categories Integrate categories to build theoretical framework
Process 5	Reaching closure	Theoretical saturation when possible	Ends process when marginal improvement becomes small

5.1 Interpretation

Over 200 codes were generated and 19 independent, contextual concepts relating to collective improvisation were identified. Each unit of analysis was analysed independently. From analysing the concepts, it was discovered that collective improvisation was more conceptually dense, i.e. occurred in many instances on the operational based domains listed in ISO 17799. A summary of results that analysed the level of conceptual density is shown in **Table 3** below.

Table 3. Mapping of Concepts with Collective Improvisation

Units of Analysis Activities related to;	**Sub categories** **(Collective Improvisation)**	**Core Categories**	*Conceptual Density of Concepts*	*Concepts*
1 **Assets control**	☑	**Strategic**	1	***Being practical***
		Tactical		
		Operational		
2 Information Architecture Security	☑☑☑	**Strategic**	3	Exceptionality, Being inventive, Rational adoptive
		Tactical		
		Operational		
3 Information Security Policy	☑	**Strategic**	1	Being quick-witted
	☑	**Tactical**	1	Lateral thinking
		Operational		
4 Event Monitoring		**Strategic**		
	☑	**Tactical**	1	Being ingenious
	☑	**Operational**	1	Being capable
5 Governance and Regulatory Compliance	☑☑	**Strategic**	2	Getting by, Being practical
		Tactical		
		Operational		
6 Business Continuity	☑☑☑☑	**Strategic**	4	Being quick-witted, Being innovative, Lateral thinking, Being ingenious
		Tactical		

Units of Analysis Activities related to;	**Sub categories** **(Collective Improvisation)**	**Core Categories**	*Conceptual Density of Concepts*	*Concepts*
	☑☑☑☑☑	**Operational**	5	Being resourceful, Managing, Being inspired, Quick reaction, Exceptionality
	19		*19*	

5.2 Axial Codes: Establishing the Principle of Self Policing by Substituting Frameworks

Tentative findings reveal that collective improvisation is most pronounced in activities related to operational activities (specifically business continuity) in governance. Collective improvisation was particularly expressive in *self-policing* where practitioners were at operational level collectively vigilant in extending *self-policing* procedures to deter, quickly investigate and contain threats to information. Using Axial Coding the researcher was able to draw relationships between various core categories. This enabled the researcher to come up with the diagram below. **Figure 1-2** shows the relationships between the units of analysis and the core categories (Strategic, Tactical and Operational).

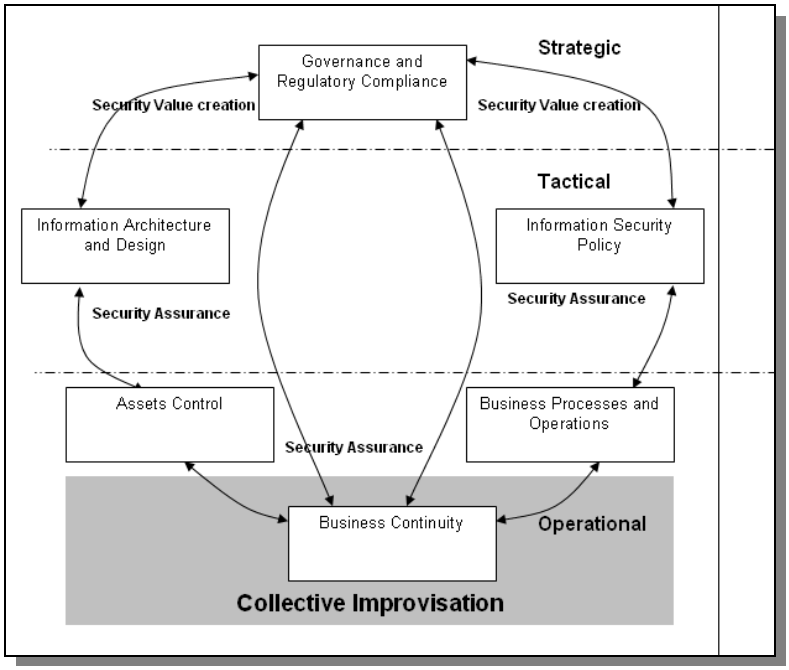

Figure 1-2 Relationship between Categories: Conceptual Density of Collective Improvisation

Figure 1-2 illustrates the conceptual density of collective improvisation as exemplified in areas where practitioners collectively engaged innovatively. Deeper insights reveal that the internalized knowledge of these practitioners was expressive in these innovative engagements temporarily substituting frameworks with their own *self-policing* initiatives. *Self-policing* and reflexivity made it necessary for the practitioners to be adaptive to contingencies.

6 CONCLUSION

To conclude, the paper has generated new insights and suggested a holistic understanding of a wide spectrum of socio-cognitive issues related to information security governance. An important part of this discourse was introducing the idea of reflexivity and collective improvisation and the role it played in information security governance. Such a role was manifested as *self-policing.*

Through a case study research, the paper has proposed a framework for understanding collective improvisation in information security governance. By understanding the proposed framework, practitioners will be able to appreciate a multi-faceted approach to Information Security governance. As laid down by the paper, the framework proposed should accommodate reflexive ways of dealing with 'intractable problems'; away from narrow structured based approaches. Reflexivity should be accommodated in the planning, management and monitoring of information security within an organisation.

7 REFERENCES

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

Beck, U. (1997), The reinvention of Politics: Rethinking Modernity in the Global Social Order, Polity Press, Cambridge.

Burton Group. (2005) Security and Risk Management Strategies, "A Systematic, Comprehensive Approach to Information Security". Version 1.0 http://www.burtongroup.com/Content/doc.aspx?cid=644

Ciborra, C. (1999) A theory of information systems based on improvisation, in Rethinking Management Information Systems (Eds: W. Currie & R. Galliers), Oxford University Press, Oxford.

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: Oxford University Press.

Cleveland H., (1973) "Systems, Purposes and the Watergate" Operations Research, Vol. 21: 5 pp 1019-1023

Dhillon, G. and Backhouse, J. (2001) "Current Directions in IS Security Research: Toward Socio-organizational Perspectives," Information Systems Journal, Vol. 1:1 pp. 11-12.

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

Glaser, B., G. (1978) "Theoretical Sensitivity: Advances in the Methodology of Grounded Theory", Sociology Press, CA.

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 pp. 153–172.

Innes, R., (1999) “Self-Policing and Optimal Law Enforcement When Violator Remediation is Valuable” Journal of Political Economy Vol 107:6 pp. 1305-1325
Kotulic, A.G. and Clark, J.G. (2004) “Why there aren’t more information security research studies”, Information & Management Vol. 41:5 pp. 597-607.
National Institute of Standards and Technology (NIST): US Department of Commerce “Risk Management Guide for Information Technology Systems” Special Publication 800 -30
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
Ogus, A. (2000), “Self-regulation”, in B. Bouckaert et G. De Geest (eds.), Encyclopedia of Law and Economics, Volume V: The Economics of Crime and Litigation, Edward Elgar, Cheltenham, pp. 587-602.
Orlikowski, WJ (1993) “CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development” MIS Quarterly Vol. 17:3 pp. 309-340
Perry L.T., (1991) “Strategic Improvising: How to formulate and Implement Competitive Strategies in Concert” Organisational Dynamics (19:4) pp. 51-64
Sarker, S., Lau, F. and Sahay, S. (2001), “Using an adapted grounded theory approach for inductive theory building about virtual team development,” The DATA BASE for Advances in Information Systems Vol 32:1 pp. 38-56.
Schultz E. (2005) “Security dilemmas with Microsoft's Internet Explorer”. Computers and Security, Vol 24:3 pp. 175-176
Scribner, S. (1984) Studying working intelligence. In B. Rogoff & J. Lave (Eds.), Everyday Cognition: Its Development in Social Context pp. 9-40. Cambridge: Harvard University Press.
Siponen, M., T. (2000) “A Conceptual foundation for organisational Information security awareness”; Information Management and Computer Security Journal Vol 8:1 pp 31-41.
Straub, D.W. and Welke, R.J., (1998) ‘Coping with Systems Risk: Security Planning Models for Management Decision Making’: MIS Quarterly, Vol. 22:4 pp. 441-464.
Strauss, A., (1987) “Qualitative Analysis for Social Scientist” Cambridge University Press, Cambridge UK.

Strauss, A. and Corbin, J. (1998) “Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory” Sage Publications, Thousand Oaks, CA.
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.
Urquhart, C. (1997), “Exploring analyst-client communication: using grounded theory techniques to investigate interaction in informal requirements gathering”, in Lee, A.S., DeGross, J.I. and Liebenau, J. (Eds), Information Systems and Qualitative Research, Chapman & Hall, London pp. 149-81.
Von Solms, B., Von Solms, R., (2004) “Ten deadly sins of security management” Computers & Security Vol. 23 pp. 371–376.
Von Solms B and Von Solms R (2005) ’From Information security to…business security’? Computer and Security Vol 24:4 pp 271-273.
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.
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.