International Journal of Business and Social Research
Volume 05, Issue 08, 2015

On Information Systems Security and when it Matters to Collectively Improvise: A Case in South Africa

Kennedy Njenga[1]

ABSTRACT

Research regarding information systems security concerns in organizations constantly focuses on the 'hard', rational and objective approaches to managing and mitigating security risks. Such research is often devoid of utilizing the 'soft' qualitative social-constructive approaches to understanding risk. This article attempts to fill this gap and presents interesting insights where these 'soft' approaches can be used as lenses to understand the management of information security. The phenomenon of improvisation and specifically collective improvisation is introduced. The research problem is that little is known about how collective improvisation is manifested in organizational settings and more importantly, how collective improvisation assists in managing information security risks. A qualitative research was therefore undertaken in South Africa, using a single case study to resolve this. Qualitative data was collected and hermeneutical exegesis techniques employed to analyses and interpret data. The key findings reveal that indeed collective improvisation was present in the case selected and manifested in unique ways that were aimed at unravelling conflicting information security challenges that this organization faced. The article discusses what these findings mean to the scholarly and practice community.

Keywords: Collective improvisation, exegesis, hermeneutics, Information systems security.
Available Online: 30th August, 2015.

1.0 INTRODUCTION

Research regarding information systems (IS) security concerns in organisations is often focused on the 'hard', rational, objective and technical approaches which assumes risks are predictable, measurable, persistent and should be managed on the basis of the probability theory (Baskerville, 2005a). There is however a growing trend in information systems security research to move away from these hard approaches and to consider the 'soft' social-constructive approaches that deal with security issues (Spagnoletti and Resca 2008). Social-constructive approaches rather than hard technical problem solving approaches in information system are increasingly being considered to be important lenses

[1] University of Johannesburg, South Africa. Email: knjenga@uj.ac.za

when considering information systems security research (Walsh, Kefi and Baskerville, 2010; Baskerville, 2005b).

One such soft approach which forms the main pillar of this article is that of understanding improvisation within the domain of information systems security. Indeed understanding how practitioners have been improvisational, innovative, creative and artistic has been addressed by various works (Stoll, 1989; Bishop, 2002; Winkler, 2007; Njenga and Brown, 2012).

What is different and unique with improvisation within the context of this article is the apparent collective nature that this phenomena is increasingly being perceived in South Africa. Collective, because importantly in South Africa's history, between the periods 1974 and 1984 the country faced increased competition and repression which co-related strongly with increased rate of collective action (Oliviera, 1991). The tendency for labour and practice to increasingly work as collective units, termed '*ubuntu*' continues to intensely manifest and is still retained within organisational settings (Newenham-Kahindi, 2009). This article considers collective improvisation from the lens of collective flexibility, collective initiative and collective work pressure (Cunha and Cunha, 2001).

1.01 RESEARCH PROBLEM

Many South African organisations and practitioners, face intense information security challenges and pressures and do not necessary have the right resources and skills to employ rational, objective and technical approaches towards managing the security of organisational information systems. Information security practitioners have thus tended to work creatively and collectively (collective improvisation) to resolve and unravel conflicting information security challenges (Grobler *et. al.,* 2011). Little is known about how collective improvisation is operationalised to mitigate against security risks and conflicting challenges. Little is also know regarding how collective improvisation is manifested by security practitioners in these contexts. It follows therefore that the research objective is to consider the following pertinent issues:

1. The extent to which improvisation is manifested as 'collective' and what this means to South African organisations.
2. How the phenomenon of collective improvisation has shaped practice in the management and mitigation of information security risk within South Africa organisations.

1.02 RESEARCH QUESTIONS

The objective of this article is to provide deeper insights regarding the collective nature of information systems security practitioners in South African organisations. In addressing the research objectives, the following are explicit research questions that provide clarity on the research work.

1. How collective improvisation is manifested and made evident when information systems security practitioners manage and mitigate threats to information systems in their organisations?
2. How does collective improvisation impact the security posture of South African organisations?
3. How would collective improvisation be addressed in these contexts so that information systems security practitioners are better placed to mitigate and manage security threats more effectively?

1.03 METHODOLOGY

In an attempt to resolve and answer the above questions, a qualitative research was undertaken and focused on one case deeply. The reason for an in-depth case study was because of the consideration that collective improvisation would be perceived as occurring within its social contexts and of the rich qualitative data that this case would provide. In-depth interviews were carried out in this case and data transcribed. Hermeneutical exegesis was applied to qualitatively examine and interpret this data. From

data analysis it was revealed that indeed collective improvisation was present and manifested in unique ways that were aimed at unravelling conflicting information security challenges that this organisation faced.

1.04 OUTLINE

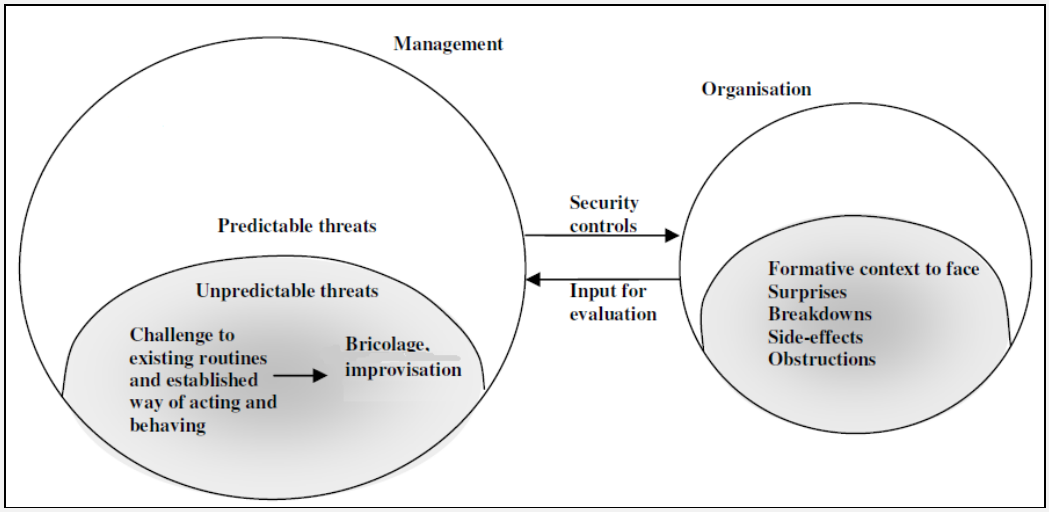
In presenting the research finding of the in-depth case study, the article is divided into four sections. The first introductory section of this article has presented the phenomenon of collective improvisation in information systems security within the contexts of South African organisations. The section that follows gives a more detailed background on collective improvisation in information systems security while providing a conceptual development of important arguments. The third and fourth sections discusses the methodology. The penultimate sections five and six discusses empirical findings and provides the implication of the research work to practice in South Africa. The final section concludes this the article.

2.0 LITERATURE REVIEW AND CONCEPTUAL DEVELOPMENT

Spagnoletti and Resca (2008) in citing (Ciborra, 2002) talk of the notion of drift which represent a phenomenon that can affect both technologies and people. According to Spagnoletti and Resca (2008), the presence of unpredictable threats in IS security requires that practice and management adapt different perspectives to maintain IS security. They call this a duality of approach to IS security. This sort of duality requires a specific epistemological approach.

In this scenario, there are two intertwined dynamics (the duality) at play. On one hand, the technology is open to new re-inventions by users and on the other through unexpected interventions, tinkering and improvisations, outlines a new way of technology adoption. In trying to understand the socio-organisational dynamics in organisations, such as interventions, tinkering and improvisations, Spagnoletti and Resca (2008) have developed a model for a subjective and interpretative understanding of these dynamics. They see such a model as an "*engine of positivist understanding*". The two intertwined dynamics (dualities) in IS security as shown in Figure 1 below are based on predictability and unpredictability of IS security threats on which formative contexts are built upon.

Figure 1: The duality of IS security (Adopted from Spagnoletti and Resca 2008).



The center of attention on this article is the left side of the stated duality in IS security. From **Figure 1** it is noted that within IS security management, unpredictable IS security threats often challenge existing routines and establish new ways of behaving such as bricolage and improvisation. **Figure 1** calls attention to improvisation in IS security management in the light of many vigorous and malevolent

adversaries, turbulence and unpredictability in the IS environment which create circumstances where IS security practitioners are hard pressed to improvise.

According to Cunha and Cunha (2001), the approach to *collective improvisation* in organisations is primarily based on three principles. The three principles include; (1) Plan to remain flexible; (2) Reliance on structure to promote initiative (3) Use pressure to boost creativity. It should be noted that the above three principles have broader implications for IS security and are more likely to change than to be followed rigidly. These broader implications relate to; (a) *consideration towards proficiency and discipline*; (b) the deliberate *encouraging spontaneous activities* that are inconsistent with prior plans (Kamonche *et al.* 2002); (c) *Logic of responsiveness* in the face of uncertainty and unpredictability that make prior plans irrelevant or incomplete (Kamonche *et al.* 2002); and (d) *lots of change in the current environment* (Kamonche *et al.* 2002).

When extending collective improvisation and meaning-making in IS security, the article explores hermeneutically how individuals acting in collaboration arrive at sufficient understanding that yield common insights aimed at supporting IS security initiatives. The concept of collective improvisation looks at meaning attributed towards "*shared or common responses, significations or intentions… the interpretive and representational processes that underlie human conduct*" (Maines, 2000). The idea of collective reflections and shared responses towards innovation and problem solving by practitioners is not new to IS security. Scholars have realised the fundamental importance of coordinated information security interaction in an organisation. Albrechtsen and Hovden (2010), develops on the idea of collective and shared responses by practitioners in organisations, and has argued that participation and reflection by teams of practitioners are likely to create advantageous information security conditions such as motivation, improved quality of technological solutions and reduced levels of risk.

It may be noted that organisational structures that enable and encourage collective and shared responses are much more reflexive and more often improvised than usually recognised. Research has suggested that collective interactions among people who are improvising frequently produce *collective improvisation* (Cunha 2004; Crossan and Sorrenti 1997). Cunha (2004) has examined Collective Improvisation in organisations and see this as **'***the combined effort of several individuals/organisations*'.

The exemplification of collective improvisation in practice is best illustrated when Conficker, a botnet is considered and how practice has dealt with this issue. Conficker, currently one of the largest currently active botnets in cyberspace, is a self-propagating worm that uses a Remote Procedure Call (RPC) buffer overflow to push the code onto a Windows machine. The potential for the Conficker botnet to do significant damage to individual Internet users, corporations, governments or even critical Internet infrastructure leads many to rank it as one of the largest and most serious cyber security threats of the past decade. The Conficker Working Group (CWG) was created, and remains, an ad-hoc organisation formed collectively by private sector corporations, groups and individuals to counter the Conficker malware threat. The group is seen as the largest collective security effort ever taken on by private industry and individuals without any official sponsor or structure.

It can be argued that the collective reflection of the Conficker Working Group in dealing with the Conficker botnet is a fundamental attribute for advancing experiences and knowledge between practice. In this case, collectivism is regarded to be important for information security work, in view of the fact that it is possible to encourage positive common insight (Albrechtsen and Hovden, 2010).

2.01 COLLECTIVE IMPROVISATION TYPOLOGIES: BRICOLAGE, INNOVATION, RATIONAL-ADAPTATION

Bricolage

Cunha (2004), states that many organisations tend to forget how much improvisation and **bricolage** are required to complete daily tasks. According to Cunha (2004), bricolage is facilitated '*by the ingenious*

use of intimately known materials'. Spagnoletti and Resca (2008) state that bricolage represents '*the capacity to tinker with the resources available'*. In bricolage, resource components are combined according to the needs of a specific context. It is as a result of this new re-combination or resource components that contribute towards new ways of acting. It is this way of acting that technology and practices can be re-interpreted. While Spagnoletti and Resca (2008) (in their model, **Figure 3**) considers bricolage and improvisation as distinctly separate entities, Cunha (2004) considers the major typologies or dimensions of *improvisation* as constituting (1) *impromptu* action in an organisational context (the article considers being *impromptu* as being *rational-adaptive*), and (2) bricolage, or the ability to draw on the available material, cognitive, affective and social resources, in order to solve the problem at hand. The article follows on Cunha`s (2004) definition. One other typology of improvisation is innovation which is discussed in the following section.

Innovation

By using empirical evidence, formal definitions of how organisations *improvise* have been developed (Moorman and Miner 1998). Miner *et al.,* (2001) have conceptualised organisational improvisation as it unfolds and perceive it as "*drawing on available material, cognitive, affective and social resources".* They equate improvisation with a form of **innovation** and suggest '*innovation is a necessary feature of improvisation"* (Miner *et al.,* 2001).

Rational-Adaptive

Improvisation can also be elucidated as simultaneously **rational** and **adaptive** and takes cognisance of rational choice and behavioural adaptation as confirmed by Doherty *et al.* (1999). On one hand, **rationality** is reflected as being (a) highly formalised; (b) applying structure and comprehensiveness in the making of decisions; and (c) focusing on control (Doherty *et al.* 1999; Segars and Grover 1999). On the other hand **adaptation** is reflected as being; (a) frequently informal; (b) entailing broad participation; and (c) flexible and loosely integrated (Segars *et al.* 1998; Doherty *et al.* 1999).

Hermeneutical exegesis is applied to explore, examine and interpret these three typologies (bricolage, innovation and rational-adaptation) in a socio-organisational setting that characterise practitioner's management of security in information systems. Hermeneutics and exegesis is discussed in the next section.

3.0 HERMENEUTICS AND EXEGESIS

Hermeneutics is seen as the art of interpreting text (Gadamer 1976) and is popular in application and use in Information Systems research (Borland, Newman and Pentland 2010; Trauth & Jessup 2000). While hermeneutics refers to the theory of interpretation, exegesis applies the techniques for doing the interpretation. Within the hermeneutical circle, there are two realms to consider; the textual realm and the social realm. Both these realm run parallel to each other. Textual criticisms dwell on the textual realm and can be defined as "*a method that seeks to ascertain the wording of the original*". Redaction criticism belongs to the social realm and can be defined as the interpreter's "*ability to trace the form and content of material used in social context or in some way to determine the nature and extent of social activity*" (Norman 1969).

Philosophical hermeneutics (Gadamer 1976), has primarily focused on the act of interpretation as exemplified by Heidegger (1962), who saw interpretation as a primary mode of human existence. Gadamer (1976) argues that individual prejudices are essential in any understanding and states that "*Prejudices are biases of our openness to the world*" (Gadamer 1976:9). In a purely classical approach to hermeneutics, the researcher cannot escape from prejudices since these lie at the heart of experience. The hermeneutical approach therefore considers reflectively the ways in which these prejudices impact the meaning of a text, or action. As Gadamer (1976:38), notes "*reflection on a given pre-understanding brings before me something that otherwise happens behind my back*". An important aspect of the hermeneutic approach is that of the hermeneutic circle which extends the analysis to the social realm of action. In the hermeneutic circle, the researcher progresses between understanding a part (e.g., a

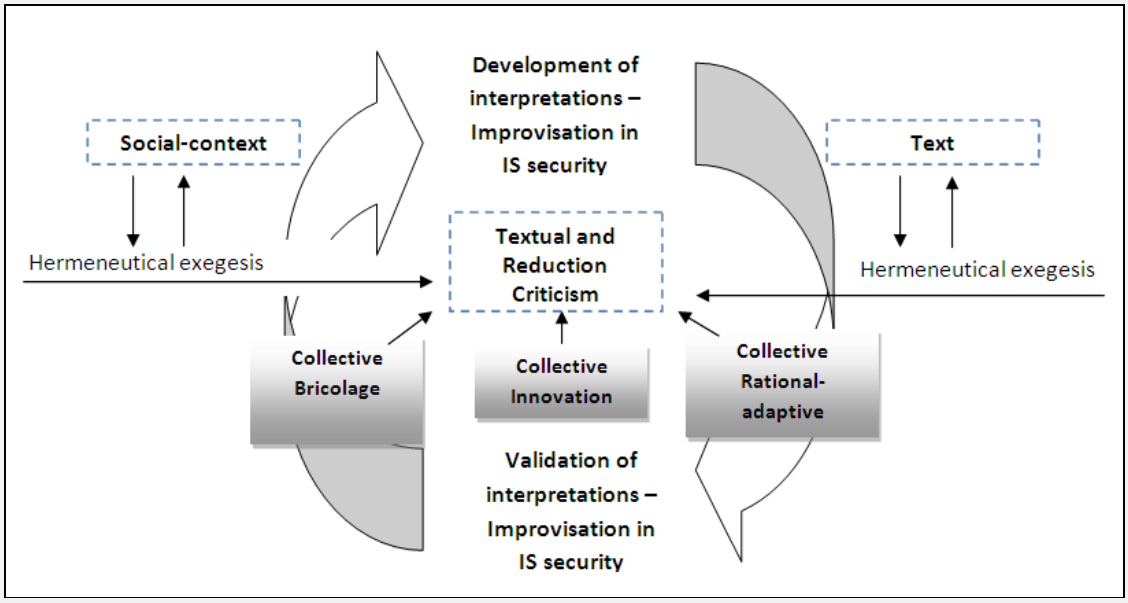
word or phrase) with respect to the whole (e.g., an entire text), and understanding the whole by grasping its composite parts. This continuity or moving back and forth is represented as the circle.

3.01 CONCEPTUAL FRAMEWORK: HERMENEUT'S UNDERSTANDING

Based on the above literature discussions on collective improvisation and hermeneutics, the researcher (the hermeneut), developed a conceptual framework for exemplifying collective improvisation in IS security using hermeneutical exegesis. Literature shows that collective improvisation has three dimensions (typologies) namely, bricolage, innovation and rational-adaptation. Within the context of IS security these three can be hermeneutically interpreted in context, on the basis of their broader implication towards IS security in the four ways mentioned previously.

Meaning-making of collective improvisation in IS security can be applied in the proposed framework in Figure 2. The proposed framework in Figure 2 below shows recursive dialectic between developing exegesis interpretations (textual criticisms and redaction criticisms) and validating interpretations within text and social-context (Hansen and Rennecker 2010). In this case, an interpretation would be based on the researcher's understanding of improvisation in its three dimensions (typologies) in IS security.

Figure 2: Using Hermeneutical Exegesis to understand Collective improvisation in IS security (Adopted from Hansen and Rennecker 2010)



The interpretation from Figure 2 above would include understanding the meanings of words or phrases in IS security used by practitioner (text) and the nature of an extemporaneous action or decision as depicted in discussions with IS security practitioners (social-context). Validation of meaning would entail appropriateness of an extemporaneous IS security action in light of the context (redaction criticisms) (Hansen and Rennecker 2010). The way this is done is discussed in the methodology section.

The processes employed by the researcher included applying the framework described in Figure 2 to generate exegesis interpretations (textual criticisms and redaction criticisms) on presence of bricolage, innovation and rational-adaptive text and social-context. This involved recursive dialectic between the exegesis interpretations and the implication towards IS security. The approach was done in tabular format as shown in Table 1 below.

Table 1: Exegesis interpretations towards finding Implication of improvisation in IS security

Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collective Improvisation (Textual and Redaction Criticisms)**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage				
Collective Innovation				
Collective Rational Adaptive				

4.0 METHODOLOGY

This section builds on the previous sections and describes the methodology employed for this empirical work. A single case study approach (of a large private organisation) was used because the study involved the examination of a complex social phenomenon.

4.01 SINGLE CASE STUDY

The organisation's Information Security department is responsible for co-coordinating secure distribution of real-time channels for its critical applications. Since the organisation offers financial services, it places importance on working within a strict regulatory environment. The organisation had been conducting the following IS security activities;

a) Controlling of access to critical Information;
b) Maintaining a sound Information security architecture;
c) Development of Information security policies;
d) Monitoring of Information security events;
e) Ensuring IT governance and regulatory compliance; and
f) Performing disaster recovery and business continuity tasks.

The purpose of these exercises as explained to the researcher was to guarantee information security to all its partners, customers and stakeholders, while ensuring the highest degree of protection from hostile attacks. The Information Security and Business Continuity Department was mandated to ensure that there was minimal interruption of critical production networks, applications and especially data. The primary objective of this department was to ensure applications were run in a secure way, protected from attack (external or internal). It was explained that this was to be accomplished through comprehensive information security auditing and assessments. Fundamental to these assessments was an IS security approach designed to: probe and validate the organisation's information security state of applications through penetration testing and vulnerability assessments; review the on-going information security practices, policies, and processes; manage information security posture in the context of the information security industry best practices, baselined against industry standards.

4.02 DATE COLLECTION AND INTERVIEWS

The primary data consisted of a series of 11 in-depth interviews on the organisations middle level IS practitioners. All interviews were tape recorded. The exegetical techniques employed from the transcripts was twofold; namely that of *textual criticism* and that of *redaction criticism* (Borland *et al.* 2010). For purposes of hermeneutical exegesis, each interview was transcribed verbatim in writing and textual criticism followed. In addition, notes were taken (redaction criticism) as the interviews progressed. The interviews were conducted for 60 to 90 minutes per session. This generated close to

700 transcript minutes for data analysis. This research work, involved translation of transcripts (original language and vocabulary used by information systems security interviewees) which was replaced (conceptualisation and generating new concepts) by language and vocabulary from the researcher. This interpretation yielded new insights and understanding of improvisation in information systems security. This interpretive translation was seen as vocabularies testing vocabulary used against text. Indeed from the research, there seemed to have been a gap between vocabulary of tradition and that of practice. Hermeneutical exegesis was applied to bridge this gap. Within the hermeneutical interpretation, there was an open and ongoing hermeneutic conversation with *in vivo* words from information systems security practitioners. Hermeneutical Exegesis from transcripts was applied in the following areas:

- Discussion regarding control of access to Information
- Discussion regarding Information security architecture
- Discussion regarding application of Information security policies
- Discussion regarding monitoring of Information security events
- Discussion regarding normative frameworks - IT governance and regulatory compliance
- Discussion regarding disaster recovery and business continuity

Textual criticism involved transcribing an accurate version of what was originally said by the IS security practitioner in each of the discussion areas highlighted above. In *Redaction criticism* the researcher established how the information security practitioner's personal characteristics and actions in the context, affected the meaning of what they were saying. This hermeneutical interpretation relied on the principles of the hermeneutic circle (Klein & Myers, 1999) where *in vivo* words used by information security practitioners were examined in detail. The examination was in light of the larger sense of the whole (theory), and where there was a tracking back and forth between detail and a whole, towards reciprocal validation. The researcher ensured that the whole was depended on the detail and *vise versa* for plausibility. The hermeneutical interpretation used in this paper considered that buried deep within the *in vivo* words of the information security practitioners were generative structures (unconscious ideas regarding collective improvisation), operating behind those words to which exegesis techniques unearthed true meaning. Levi-Strauss (1963) has also outlined and argued for this approach (uncovering hidden meaning).

In order to explore how *redaction criticism* was used to add richness and understanding of improvisation in information systems security, we applied this technique from transcripts obtained from the single case study mentioned above. The **Table 2** below shows how the hermeneutical and exegesis techniques were applied.

Table 2: Exegesis techniques: Using Textual and Redaction criticism to identify improvisation

STEP 1 **Textual Criticism**	**STEP 2** **Hermeneut Metrics On Collection Improvisation**	**STEP 3** **Redaction criticism: Interpretation and creation of concepts**
This step involved, the researcher establishing an accurate version of what was being said by the IS security practitioner using a coding scheme (Schegloff & Sacks, 1974). This involved using commas, semi-colons and quotation marks where appropriate.	This step involved writing memos based on a mutual understanding of the unique combination of interviewer and interviewee context that explained either of the following; ▪ Collective **bricolage** ▪ Collective **innovation** ▪ Collective **rational-adaptation**	This step involved "looking for a vocabulary in which a puzzling object could be related to other, more familiar objects, so as to become intelligible" (Rorty, 1982). This involved understanding how behavioural characteristics were shaping words. Interpreting and using own words to describe context.

Table 2 shows that the first step in the process was to establish an accurate version of original words from the practitioner. Textual criticism was applied to transcripts, and this involved a few cycles of comparing recording to transcripts. A coding scheme used by ethnomethodology researchers (Schegloff & Sacks, 1974) was adopted as follows;

/ Indicates upward intonation
(. . .) Indicates a pause proportional to the number of dots
() Indicates something said but not transcribed
(word) Indicates probable, but not certain transcription
but Indicates emphasis
emPLOYee Indicates heavy emphasis
(INT:) Comments from the interviewer

Once the process of *textual criticism* and *redaction criticism* was done, certain theoretical ideas began to emerge to the researcher which appeared central to the study of improvisation in IS security. These ideas were documented in tabular format. **Table 3** below, shows an example of how this was done.

Table 3: Textual criticism and Redaction Criticism for Single Case Study

STEP 1 (Textual Criticism)	**STEP 2 (Hermeneut Metrics)**	**STEP 3 (Redaction Criticism-Finding Common Vocabulary)**
(…) so we qUICKly had to make (INT: create)*(…) a few more categories (…) so it doesn't just get as simple as you just hAVIng internet access (..) and you don't gET THIs..* (but rather) *you having internet access (..)and(..)you belong to marketing(…)and you belong to IT(.)*	Profiling users based on user activities was found to be critical. However, it was the nature of the profiling as observed that was to be found interesting. Multiple users had multiple requirements. The creation of extra categories outside of the normal categories was considered as having elements of **bricolage** since this had never been done before. i.e. new ways of defining categories that allowed for **innovative** information access.	Implies presence of both bricolage and rational-adaptive.
(..) to give to the people ()that they gave(…)and got the ones that (**were**) *broken…they had to tHINK quick...and MAKe that kind of a judgment(…)*	Practitioners were initially not thought of as being **rational-adaptive** when they re-issued old laptops to ensure processes continued to run; no one could predict that their quick judgment would later prove useful	Implies presence of rational-adaptive.

In this technique the researcher established how the information security practitioner's personal characteristics and actions in context influenced the meaning of what they were saying. Using redaction criticism the researcher studied the socio-cultural behavior and action of IS security practitioners with the concern primarily being how this was shaping what they said. There was recognition that their world view shaped what they said.

5.0 TEXTUAL CRITICISM AND REDACTION CRITICISMS ON IMPROVISATION

Table 3 shows how hermeneutic exegesis was used to understand the various typologies (bricolage, innovation and rational-adaptive) of *collective improvisation* through discussions held with the information security practitioners in the six discussion areas. IS security practitioners were able to relate to the questions being asked and had a clear recollection of their everyday tasks. A good flow of information was sought and healthy discussions were held. The six discussion areas presented in the section below expound on what was said.

5.01 DISCUSSION REGARDING CONTROL OF ACCESS TO INFORMATION

From the discussions held, new insight into the process of IS security management was evident particularly in how practitioners managed information access and data control. A summary of findings from the discussion is shown on Table 4 below.

Table 4: Hermeneutical exegesis on control of access to Information

Summary: Discussion regarding control of access to Information				
Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collection Improvisation**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage			☑	
Collective Innovation				
Collective Rational Adaptive		☑		

Table 4 can be explained as follows: Although there were specified procedures that prescribed acceptable ways on how IS security practitioners were treat information assets, the discussions revealed that this was adhered to only up to a certain point.

> "Roles (**end users' roles**) are specifically sPLIt into two areas(..) technical response(..) and the pROCess, procedures and people element."
>
> "(…) 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 (…)"

Textual criticism shows emphasis on certain areas. Hermeneutically this was interpreted to mean that 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 (redaction criticism). This was in context to what was happening could be possible if there was a culture which encouraged *spontaneity*. This was considered to be **rational-adaptive** with implications of spontaneity. A check was placed in **Table 4** above for this interpretation.

In one particular instance, it was noted that access to sensitive information was granted spontaneously to a user who requested such access:

> (…) so we qUICKly had to make (INT: create)(…) a few more categories (…) so it doesn't just get as simple as you just hAVIng internet access (..) and you don't gET THIs.. (but rather) you having internet access (..)and(..)you belong to marketing(…)and you belong to IT(.)

This act of spontaneity in determining access levels demonstrated the need to address information access needs quickly by a tinkering process. The researcher hermeneutically interpreted this to mean **bricolage.** At the heart of this kind of *collective improvisation* was the ability of practitioners to react quickly and ingeniously to overcome emergent constraints and was perceived as logic *of responsiveness*. A check was placed as shown on Table 4. Textual criticism and redaction criticism was applied to the five other sets of discussions. Exegesis on these other discussions follows a similar approach. The next sections show this.

5.02 DISCUSSION REGARDING INFORMATION SECURITY ARCHITECTURE

A summary of findings based on these discussions is shown below in Table 5.

Table 5. *Hermeneutical exegesis on information security architecture*

Summary: Discussion regarding Information security architecture				
Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collection Improvisation**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage		☑	☑	
Collective Innovation				
Collective Rational Adaptive				

From discussions it was revealed that the organisation's architecture forum was primarily responsible for the organisation's security architecture. This as evidenced by the following text:

> "We hAVE GOT the Architecture forum, which sits under [name withheld] (…) and uhm, we also have (another forum), which (..) I'm more iNVOLVed in (…) in making sure that there is compliance architecture (…)"

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 (…)"

Through redaction criticism it seems that there are indications that in certain circumstances there were no clear guidelines to follow, hence "*(…) soMETimes we don't know IF it is the rIGHt thing to do(..)". The pUT together our plan* denotes bricolage. The element of spontaneity and logic of responsiveness is also noted as shown on Table 5.

5.03 DISCUSSION REGARDING APPLICATION OF INFORMATION SECURITY POLICIES

Table 6. *Hermeneutical exegesis on information security policies*

Summary: Discussion regarding Information security policies				
Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collection Improvisation**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage		☑		
Collective Innovation				
Collective Rational Adaptive		☑		

Table 6 is explained as follows: One information security practitioner was asked who (between employees and third parties), played a greater role in helping define the organisation's information security needs and policy. It was revealed that the role was split:

> "(..) there is an equal level of contribution(…) in bALANCing the nEEDs of the company and tHOSe advised by third parties(..)."

The researcher noted the emphasis on the words "balancing" and "needs". It was revealed in the discussions that in matters of prioritising for information security based on policies, this often called for tinkering. One practitioner had this to say:

> "(…) and oBVIOUsly now when we rEFLEct on it (policy) (…) it has nOT been too bad on business(..) but now when we hIT certain aREas(..) is that(..) we have to make sOME kind of adjustments (…) because there are so many applications out there (…) and the thing is that(..) to be working(…) these neEDs to run on the aDMinistration rights of the machine (…)"

The researcher was able to interpret a degree of thorough intuitive and technical understanding on the part of the information security practitioners in making tinkered adjustments as was seen as **rational-adaptive** only possible in a culture that encourages spontaneity. Another instance that demonstrated tinkering and **bricolage** was evidenced in the text below.

> "(…) so we actually mADe prOVisions, that we could do it (amend policy) when we looked at the group policy (…) on administration rights issues(…)"

The hermeneutical interpretation is that while IS security practitioners were able to appreciate policies in place they still encouraged themselves to be (or rather the culture there was to encourage) spontaneity.

5.04 DISCUSSION REGARDING MONITORING OF INFORMATION SECURITY EVENTS

The researcher asked one practitioner whether there were policies for reporting incidents, and whether there were procedures to follow as laid down by the organisation when reporting incidents, he replied as follows:

> "(..) yES (…) incidents are generally rEPOrted to IT risk management or via our external service provider through their network monitoring mechanism(..)"

It was also reported that there were mechanisms in place to ensure that most of the critical information security incidents were captured and reported. This was explained by one information security practitioner as follows:

> "(..) there is a formal meeting held monthly(…) however (..) if serious breaches are detected(..) emergency meetings are convened(…) there are also automated alerts prompting us of potential threats(…) specifically eXTERnal threats(…)"

The information security practitioner also mentioned that they reported incidents while these occurred:

> "(…) (incidents) are rEPORTed as they oCCUr or detected by our external service providers(…) who monitor our network activity(…) WE have a monthly meeting to analyse incidents received(…)"

One interviewee mentioned that the monitoring process was based on set standards, and if there were deviations, then these would be reported:

> "(we carried out) particular cHECKs around [systems] abuse(…) which forms part of our information security requirements to ensure confidentiality and integrity basically at more or less operational level (…)"

Although there a significant time was spent doing textual and redaction criticism on this discussion, it was difficult to pinpoint collective improvisation in this instance. Thus **Table 7** below was left blank.

Table 7: Hermeneutical exegesis towards monitoring information security events

Summary: Discussion regarding monitoring information security events				
Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collection Improvisation**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage				
Collective Innovation				
Collective Rational Adaptive				

This was interpreted to mean that it remained difficult for practitioners to improvise when guidelines were clearly set. This could mean that improvisation was only applicable to fill in gaps where procedure regarding the monitoring process was silent.

5.05 DISCUSSION REGARDING NORMATIVE FRAMEWORKS - IT GOVERNANCE AND REGULATORY COMPLIANCE

With regard to discussions relating to IT governance and regularly compliance, the researcher noted that compliance was as a result of how IS security practitioners interpreted their own policies:

> "(…) 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 (…)"

The context of the text was that the practitioner found it easy to roll out CobiT once there was buy-in from the top. From the discussions, it seemed experience has shown that rolling out of CobiT without this specific buy-in would have proved difficult. This was logic of responsiveness that proved innovative. This interpretation is illustrated on Table 8 below.

Table 8. *Hermeneutical exegesis on normative frameworks, IT governance and regulatory compliance*

Summary: Discussion regarding normative frameworks - IT governance and regulatory compliance				
Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collection Improvisation**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage				
Collective Innovation			☑	
Collective Rational Adaptive				

5.06 DISCUSSION REGARDING DISASTER RECOVERY AND BUSINESS CONTINUITY

The discussions revealed that the organisation had put in place a process for maintaining business continuity. The challenge to the process was that there was always an unanticipated event that resulted in making practitioners think extemporaneously. This thinking is illustrated in the following incident where for the sake of continuity the practitioners made collective judgment and were forced to issue old, out of warranty lap-tops:

> "(…) thEY had to thINK quick (…) and make that kind of a judgment (…)"

During the interview It was observed that one particular practitioner (in consultation with other practitioners) used the classification/categorisation model that focused on processes from a business recovery point of view innovatively. This is evidenced by the following data incident:

> "(…) yes and (we) categorised those items (…) we sPECIFically focused on [those items], pARTICularly from a disaster recovery and also business continuity (…)"

The context of this text and discussions was that scenario planning was essential to determining business continuity and business recovery measures. However, the scenario plans did not restrict the approach to creative solutions, and the practitioners were free to expand their thinking consciously to manage these activities. That was why the researcher interpreted this as innovation. The innovation could only be possible if triggered by lots of changes in the IS security environment. From a business continuity perspective, changes were common. The hermeneutical interpretation for this instance is shown in **Table 9** below.

Table 9: Hermeneutical exegesis on disaster recovery and business continuity

Summary: Discussion regarding disaster recovery and business continuity				
Implication towards Information Systems security (ISS)- Risk Mitigation **Hermeneut Metrics On Collection Improvisation**	Encouragement of Proficiency and discipline	Encouragement of Spontaneity	Logic of Responsiveness	Turbulence/ Chaos and lots of change in IS security environment
Collective Bricolage				
Collective Innovation				☑
Collective Rational Adaptive				

6.0 IMPLICATIONS FOR PRACTICE

On the basis of the in-depth single case study provided, empirical data shows that collective improvisation manifests as joint effort and collaboration in the form of bricolage, innovation and rational adaptive. It is important to note that collective improvisation in these three forms proved to be beneficial towards the mitigation of information systems security risk in South African organisations. This is based on the observed decision points suggested by information security practitioners. The following table provide a policy framework that would signify the importance of managing beneficial outcomes of collective improvisation within organisational settings.

Table 10: Policy Framework to Encourage Collective Improvisation

Tenets of Good Information Security Practices	**Policy implication for collective management of information systems security**
▪ *Control of access to Information*	It is important to institute policies that encourage the co-operation of people through collective innovations when instituting control over access to restricted information. This is important when people are jointly given a platform to contribute to issues regarding how to best treat personal data.
▪ *Sound Information security architecture*	It is important to provide a platform for joint co-creation of a sound information security architecture.
▪ *Continuous monitoring information security events*	
▪ *Pragmatic Information security policies*	It is important to ensure that users of systems co—operate in following policy directives. Co-operation is especially important where there are different types of employees, different types of potential incidents where the involvement of everyone is necessary to prevent these incidents escalating.
▪ *IT governance and regulatory compliance*	
▪ *Effective disaster recovery and business continuity*	

Contribution

The contribution this works brings into literature is that the study of a construct such as collective improvisation is not necessarily confined in disciplines such as psychology and sociology but can be especially extended into the discipline of information systems. In this work, collective improvisation has been used as a lens to demonstrate how security practitioners could handle and manage security risk.

7.0 CONCLUSION

The appropriateness of collective improvisation in IS security proves effective provided the information security practitioners are skilled enough and are capable of utilising the best available resources. The work has presented empirical data to demonstrate this. It should be noted that for this specific case, collective improvisation served as antecedents to information security risk mitigation. It is from such observation that a policy framework (Table 10 above) that takes cognisance of collective action could be developed and extended further. The research work provide deeper insights for this to happen. While this work is specific to one case within South Africa, an extended debate into various other soft approaches to understanding information security in organisations is to be encouraged. It is hope that this work has opened up such a platform.

REFERENCES

Albrechtsen, E., Hovden, J. (2010), Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*; 2(9), p. 432 – 445.

Baskerville, R. (2005a) Information Warfare: a comparative framework for Business Information Security, *Journal of Information System Security*, 1(1) p. 23-50.

Baskerville, R. (2005b), Best Practices in IT Risk Management: Buying safeguards, designing security architecture, or managing information risk? *Cutter Benchmark Review*; 5(12), p. 5-12.

Bishop, M. (2002) *Computer Security, Art and Science*, Addison-Wesley Professional, Reading, MA.

Borland, R.J., Newman, M. and Pentland, B.T. (2010), Hermeneutical exegesis in information systems design and use, *Information and Organization* 20, p. 1–20.

Ciborra, C. (2002) *The Labyrinths of Information*, Oxford University Press, London

Crossan, M.M. and Sorrenti, M. (1997) Making Sense of Improvisation *Advances in Strategic Management* 14, p. 155-180.

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

Cunha, J.V. and Cunha, M.P. (2001) "Brave new (paradoxical) world: structure and improvisation in virtual teams" *Strategic Change* 10(6) p. 337-347.

Doherty, N. Marples, C. and Suhaimi, A. (1999) The relative success of alternative approaches to strategic information systems planning: An empirical analysis, *Journal of Strategic Information Systems* 8, p. 263-283.

Gadamer, H.G. (1976). *Philosophical hermeneutics*. University of California Press. Berkeley, CA.

Grobler, M., Jansen van Vuuren, J. and Zaaiman, J. (2011). Evaluating Cyber security Awareness in South Africa. 113-121. Available from: http://researchspace.csir.co.za/dspace/bitstream/10204/5108/1/Grobler1_2011.pdf?origin=publication_detail

Hansen S. and Rennecker J. (2010), Getting on the same page: Collective hermeneutics in a systems development team, *Information and Organization* 20, p. 44-63.

Heidegger, M. (1962), *Being and time.* (J. MacQuarrie & E. Robinson, Trans.) (1st English ed.). SCM Press, London.

Kamoche, K.N., Cunha, M.P. and Cunha J.V. (2002) "*Organisational Improvisation*" Routledge, London.

Klein, H. and Myers, M. (1999) A set of principles for conducting and evaluating interpretive field studies in information systems, *MIS Quarterly*, 23(1), p. 67.

Levi-Strauss, C. (1963), *Structural anthropology*, Basic Books, New York, NY.
Maines, D.R. (2000). The social construction of meaning. *Contemporary Sociology*, 29(4), 577–584.
Miner, A.S., Bassoff P. and Moorman, C. Organizational Improvisation and Learning: A Field Study" *Administrative Science Quarterly* 2001, 46(2) p. 304-337.
Moorman, C. and Miner, A. (1998a) Organisational Improvisation and Organisational Memory, *Academy of Management Review* 23(4), p. 698-723.
Njenga, K. and Brown I. (2012), Conceptualising improvisation in information systems security, *European Journal of Information Systems* 21 (6), p. 592-607.
Newenham-Kahindi, A. (2009) The Transfer of Ubuntu and Indaba Business Models Abroad: A Case of South African Multinational Banks and Telecommunication Services in Tanzania, *International Journal of Cross Cultural Management* 9 (1), p. 87-108
Norman, P. (1969) *What is Redaction Criticism?* Fortress Press, Philadelphia, PA.
Oliviera, J.L. (1991) State repression and collective action in South Africa, 1970–84 *South African Journal of Sociology* 22 (4), p.109-117.
Rorty, R. (1982). *Consequences of Pragmatism*. University of Minnesota Press, Minneapolis.
Schegloff, E. and Sacks H. (1974). Opening up closings, In R. Turner (Ed.), *Ethnomethodology*. Penguin, Middlesex.
Segars, A and Grover, V. (1999) Profiles of strategic information systems planning. *Information Systems Research* 10(3), p.199-232.
Segars, A. Grover, V. and Teng, J. (1998) Strategic information systems planning: Planning system components, internal co-alignment, and implications for planning effectiveness, *Decision Sciences*, 29(2), p. 303-344.
Spagnoletti, P. and Resca, A. (2008) The Duality of Information Security Management: Fighting against Predictable and Unpredictable Threats, *Journal of Information System Security* 4(3), p. 46–62.
Stoll, C. (1990) *The Cuckoo's Egg, Tracking A Spy Through the Maze of Computer Espionage,* Pocket Books, New York, NY.
Trauth, E.M. and Jessup, L.M. (2000) Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use, *MIS Quarterly* 24(1), p. 43-79.
Walsh, I. Kefi, H. and Baskerville, R. (2010) Managing culture creep: Toward a strategic model of user IT culture, *Journal of Strategic Information Systems* 19 p. 257-280.
Winkler, I. (2007) *Zen and the Art of Information Security,* Syngress, Rockland, MA.