CONCEPTUALISING THE INFLUENCE OF TACIT KNOWLEDGE IN SECURITY RISK MANAGEMENT ACTIVITIES

Kennedy N Njenga [a] and Irwin Brown [b]

[a] Department of Information Systems, University of Cape Town/ S. Africa
[b] Department of Information Systems, University of Cape Town/ S. Africa

[a] njnken001@mail.uct.ac.za, Leslie Commerce UCT, Tel +27 (21) 650 4233
[b] ibrown@commerce.uct.ac.za, Leslie Commerce UCT, Tel +27 (21) 650 4260

ABSTRACT

The concept of tacit knowledge is introduced and explored particularly by examining how it influences an organisation's security risk management activities. This exploration lends credit to validating the "soft" discursive attributes of security risk management within organisations. The theme focuses on the general aspects of information systems' exposure to security risk and conceptualises the process of capturing extemporaneous human activities that guide the security risk mitigation process. The underlying primary proposition is twofold; firstly, that there are multiple approaches to security risk management each unique in its own way that is impacted by tacit awareness, and secondly, that the risk management process is a contextual, free floating and independent construction shaped by improvised actions and tacit knowledge. What is finally outlined is that the patterns of insights that subconsciously evolve within the frame of tacit knowledge continually guide the risk mitigation process. It is proposed that the best way to capture tacit knowledge is through a security knowledge repository (*SecBase)* designed to map cognitive extemporaneous activities into this repository using an algorithm.

KEY WORDS
Security Risk, Risk Mitigation, Tacit Knowledge, Improvisation

CONCEPTUALISING THE INFLUENCE OF TACIT KNOWLEDGE IN SECURITY RISK MANAGEMENT ACTIVITIES

1 INTRODUCTION

The relevance of understanding information security risk and the risk awareness from a managerial perspective is a widely recognised IT oversight. This understanding rightly so, has generated great interest amongst information security researchers (e.g. Thompson and Von Solms 1997; Straub and Welke 1998; Siponen 2000; Von Solms and Von Solms 2005). Indeed many researchers interested in security risk at organisational level have recognized the significance of sound risk management policies that focus on clear methodologies and programmes (Von Solms and Von Solms 2005; Schultz 2005). Organisations that have modelled the Internet and ICT as part of their service infrastructure place stringent information security requirements on their most valuable assets (Smith *et al*. 2003). These requirements are precipitated by the need to control criminal and illicit transmissions/activities that arise from system vulnerabilities. Many large organisations continue to develop comprehensive approaches to information security that incorporates the complexities of their enterprises as shown by Chambers *et al* (2005). Smith *et al* (2003) considers any approach to security as deficient if the awareness of security issues is not prioritised. This imperativeness of approach has lead organisations to adopt standards and frameworks that guide the controlling, assessment and the mitigation of security risk all of which enhance security awareness through a feedback loop at the operational, tactical and strategic levels of control.

2 SECURITY RISK MANAGEMENT CACOPHONY

From a contextual perspective, organisations perceive security risk as “a function of the *likelihood* of a given *threat-source* exercising a particular potential *vulnerability*, and the resulting impact of that adverse event on the organization” (NIST SP 800-30). It follows that from this definition, numerous security risk management approaches could be used and as a matter of fact do indeed exist that help organisations assess and control risk. This is illustrated by many ways, technical or otherwise, in which organisations assess both the threat sources and the likelihood of adverse events that follow. What follows thereafter is usually the many ways to control or mitigate such threats. The significance attached to these many approaches becomes critical to security risk management particularly when consideration is given to past and present statistics on computer attacks by hackers/crackers (Forno and Baklarz 1999). Organisations should therefore understand the importance of security risk particularly when determining the levels of responsibilities to assign their resources.

2.1 Conventional Methodologies and Standards to Managing Risk

At the core of most organisations' operational, tactical and strategic levels will lie several methodologies that organisations deem suitable to meet the unique diverse and high technology risks associated with running computerised systems. These stem either from government regulations (Sarbanes-Oxley Act) or industry recommendations such as CoBIT, COSO, (Committee of Sponsoring Organisations of the Treadway, Commission, *Internal Control—Integrated Framework*, 1992), the COSO *Enterprise Risk Management Framework*, 2004, Turnbull in the UK, CoCo in Canada, KING II, in South Africa and the IT Infrastructure Library (ITIL) for IT service management (ISACA 2006).

In context, the security risk and awareness frameworks focus on explicit standards and methodologies that align to formal structures (Von Solms and Von Solms 2005; Schultz 2005). The explicit frameworks and standards are seen as value specific components of corporate governance. Formalising and adopting these standards as embodiments of effective corporate governance provides the IT governance and control objectives for the organisations' process owners.

2.2 Emergent Alternative Approaches to Managing Risk

In view of alternative perspectives, there is strong evidence to suggest that managing security risk that radiates around organisations has constantly been challenged by the emergent changes in technology, in effect making assessment and control of security risk a more complex task than naturally expected. Furthermore, there is increasing emphasis on compliance issues derived from explicit methodologies as awareness tools, while drawing attention away from actual security activities (Jackson 2006). The danger here is that getting too involved with compliance issues may not necessarily translate to improved security (Jackson 2006).

Improved security on the other hand will involve people and processes. Parker (2001) argues that information security is “a holistic process that not only includes hardware, software, but also people…” and postulates the argument that a key success factor would be a people driven approach that evaluates and selects the best responses to changing technologies and not just isolated individual technology solutions such as firewalls, intrusion detection systems (IDS) or public key infrastructures.

It should also be noted that the information security process should also consider the increased technology changes that give rise to system vulnerabilities. These vulnerabilities have been highlighted as important to due to their nature being emergent, continuous, difficult to control and highly filled with surprises (Weick 1993b; Parker 2001).

These stated attributes can be seen to cast a significant re-thinking on how the organisations use explicit methodologies and frameworks as awareness tools when consolidating security risk information. When perception shifts from attention to compliance on explicit methodologies to a people focused approach to managing security risk, it could be argued that this will immediately create awareness to the multiple approaches to security risk management, and therein lies the concern.

It could be further argued that these many approaches are affected by the level of tacit awareness and skills level of people and that;

(a) Because of the emergent technologies, any acceptable doctrine of standard approaches or methodology to security risk management will continually evolve creating new patters of insights and understanding.

(b) Skills level of people will influence the many approaches to security risk management creating a contextual, free floating and independent environmental constructions of security activities shaped by extemporaneous actions and tacit knowledge.

(c) The influence of tacit knowledge bridges the gap between the subconsciously evolving patters of security risk insights and the emergent technical problems that occur outside of explicit methodologies and standards.

3 CONTEXTUALISING TACIT KNOWLEDGE

Baumard (1999) provides the most extensive treatment of tacit knowledge in knowledge management and organisational context, the importance resting squarely on its ability to be a source of competitive advantage. An important factor to note is that people are embedded with knowledge that they are not aware of having learned (Polanyi 1966;Baumard 1999).

To understand the concept of tacit knowledge, Nonaka (1994) defines it as a "non linguistic non-numerical form of knowledge that is highly personal, context specific, and deeply rooted in individual experiences ideas, values and emotions". Tacit knowledge has also been considered "practical rather than academic, informal rather than formal…It is not accessible to consciousness awareness, unspeakable or unteachable" (Wagner and Sternberg 1985).

Thus, rather than being evident in the explicit methodologies and standards mentioned earlier, tacit knowledge will primarily manifest itself in the informal undocumented, improvised actions performed by security personnel as part of their daily work activities. To understand how improvised actions seem to draw out tacit knowledge, a brief documentation follows.

3.1 Tacit Knowledge Expressed in Improvised Activities

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" (Polanyi (1966). Ciborra (1999) reasoned that purposeful improvised activity draws from tacit knowledge, that is, knowledge that cannot easily be communicated because it is deeply rooted in a user's experience. According to Ciborra *et al* (2000) the foundation for improvised activities lies on the premise that information systems are no longer stable, discrete entities, but part of elaborate networks and information infrastructures that are subject to constant adjustments and adaptation. He considered improvised activities as "simultaneously rational and unpredictable; planned but emergent; purposeful but opaque; effective but irreflexive; discernible after the fact but spontaneous in its manifestation".

To contextualise this understanding, an extemporaneous activity in security risk management could be flexible. This flexibility positions a security risk management exercise to be "solved" now in one way, and in the future in another way and that in each way it may finely fit into the occasion. This flexibility has been the basis for the development of theoretical ideas about extemporaneous actions (Peplowski 1998; Weick 1993b), though many writers drawn much of the theoretical ideas from anecdotal or casual observation and empirical evidence (Cunha *et al* 1999).

To conclude on this brief it may be worth noting that a lot of purposeful improvised security risk activities remain undocumented and this knowledge gets "lost". The next section proposes how an organisation may retain this knowledge for future use.

3.2 Capturing Tacit Knowledge

It may be worth mentioning at this stage that tacit knowledge is inherently communicated via face-to-face interactions (Nonaka 1994) and there is need to establish a mechanism that integrates these social activities and specifically extemporaneous acts into a technological and collaborative environment. The modus operandi and challenge is to re-discover information that has already been discovered, though this information lies buried within the minds of people. One useful way of overcoming this challenge, from a socio-technical perspective, is by finding meaningful ways in which people exchange security risk knowledge and in capturing this knowledge.

Part of the tacit knowledge capturing phase would include the process of examining how the collaborative applications collate extemporaneous social activities relating to security risk management and then use technology to capture it. The integration of the social with the technical will allow for the conceptualisation of these interactions in order to extract tacit knowledge and reflect on the significance this knowledge plays in influencing security risk management activities. The motivation would be to deconstruct prior knowledge that is *ex nihilo nihil fit* (did not come from nothing) (Ng'ambi 2006).

4 ROLE OF TECHNOLOGY AND THE RE-DISTRIBUTION OF KNOWLEDGE

It can be seen that there occurs a wide range of social interaction and activities between security risk professionals within and outside organisations. Significantly, technology particularly integrated collaborative technologies that integrate other disparate technologies has aided in the interaction process. One technology of concern would be the security knowledge repository built on conventional standards (CoBIT, COSO, KING II etc) used by security professionals when managing the security risk process and how information feeds in and out of this repository. The security knowledge base or '*SecBase*' as it is referred to henceforth, would be an ideal starting point to conceptualise the knowledge capturing process.

SecBase would be conceptually mapped with people's past and new experiences, skills and interests including extemporaneous activities by a system that runs on an algorithm designed to monitor these new collaborative streams. The system would select key words relating to security risk e.g. *Risk*, *Action*, *Control*, *Virus*, *Denial of Service*, *Measures* and map these into *SecBase* thus building on the previous knowledge with emergent new knowledge. The system should support synchronous and asynchronous collaborative tools, such as Dynamic Frequently Asked Questions (DFAQs) environments (Ng'ambi 2006), threaded forums, instant [mobile] messaging using Personal Digital Assistants (PDAs), thus creating an interesting solution that would capture the knowledge of security professionals as they form direct one-to-one communication as well as in group based virtual meeting rooms. The flow of tacit knowledge would much readily be captured and contained within this system.

Implementing a collaborative technical-based but social system is well understood and evident for instance in the work of Ng'ambi (2006). He notes that such a collaborative system 'facilitates the construction and de-contraction of knowledge' and usually revolves around acquisition of new knowledge involving the construction and de-construction of prior knowledge, thus the knowledge shared being *ex nihilo nihil fit* (did not come from nothing) but "was an outcome of social structure".

The challenge of the capturing process should be in creating a security knowledge extraction algorithm that would sit between *SecBase* and these collaborative streams of knowledge or the conceptual ontology of security experts' experiences (tacit knowledge) and pulling in queries from a security professional. A proposal to overcome this challenge would be to develop mechanisms (algorithms) that automatically detect security risk concepts from a particular collaborative system by relating this information to the *SecBase* system and re-constructing new security knowledge using knowledge obtained from *SecBase.*

5 PROPOSED RESEARCH

5.1 Conceptualising the Cognitive Security Risk Frames

It would be important to address and describe the process of capturing tacit knowledge to *SecBase,* using a cognitive mapping process. Figure.1. illustrates a conceptual algorithm receiving queries from a security professional who interacts with *SecBase*. The diagram shows how the algorithm would use the inferential capabilities of *SecBase* and try to determine whether *SecBase* contains structural information that conceptually matches the query received. Emerging knowledge of *SecBase* would include mapping cognitive tacit knowledge into *SecBase*.

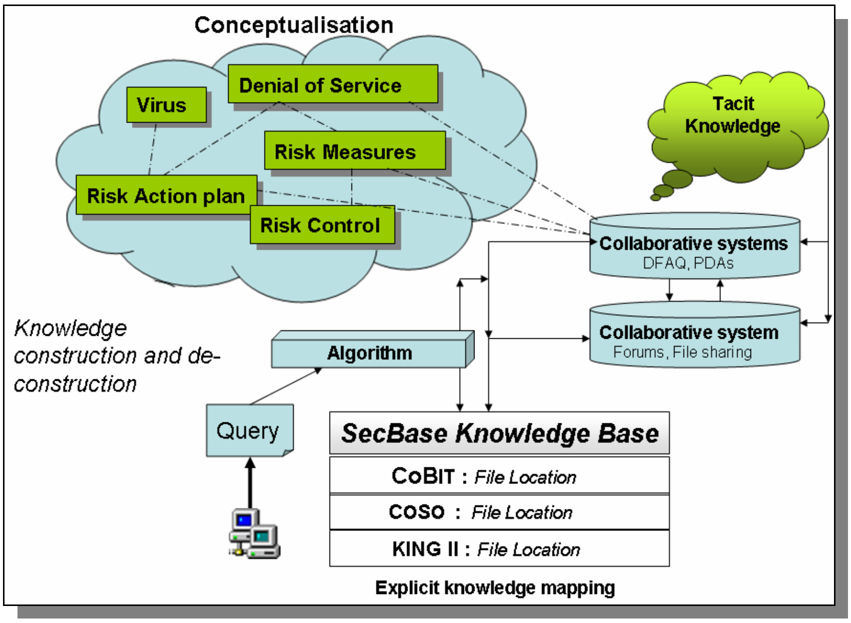

Fig 1. *Conceptualisation of Tacit knowledge and Security Knowledge Frames*

While the concern is in the capture of tacit knowledge, by for instance processing information from collaborative systems like forums, PDAs and DFAQs (Ng'ambi 2006), an important issue to consider would be the way unstructured documents sourced from these collaborative streams would be represented and processed for knowledge construction, de-construction and finally effective extraction.

5.2 Influencing Security Risk Activities

It may theoretically be argued that tacit knowledge will influence the emerging knowledge in *SecBase* and consequently the way security risk is managed by the organisation. This can be seen in Figure 2. below

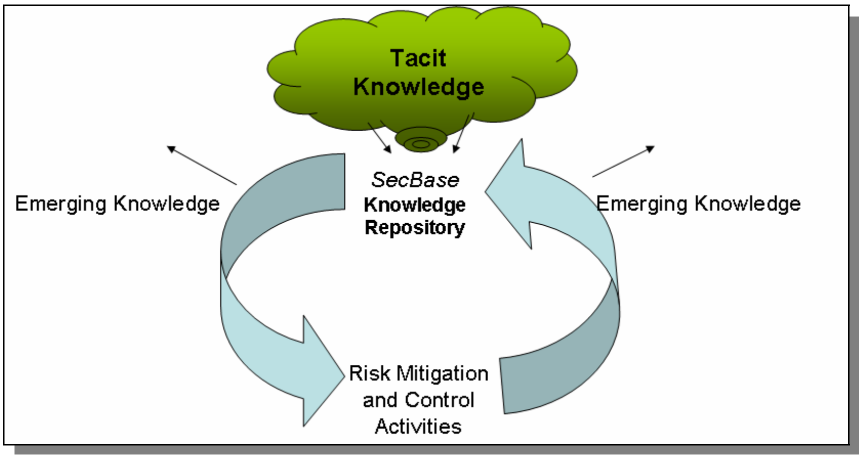
Tacit Knowledge
Emerging Knowledge
SecBase Knowledge Repository
Emerging Knowledge
Risk Mitigation and Control Activities

Fig 2. *Cyclical process of tacit influence*

Figure 2. shows the *cyclical* process of tacit knowledge and the influence it has on risk activities (control and mitigation). In the sense that experts will use collaborative technologies to communicate new knowledge and that this new knowledge will be picked up by *SecBase* repository which will further influence action. It will be noted at this stage that flexibility in security risk management activities could be of importance particularly in the event that improvised activities would fill the unavoidable gap between explicit standards and events as they arise. In such a case, improvisational action that draws from tacit knowledge can be an acceptable model to be deployed

6 CONCLUSION

While shifting attention from compliance on explicit methodologies we have introduced an alternative perspective strengthening the need to critically examine the people process in security risk management activities. Critical to these activities is the role tacit knowledge plays. In this paper, we have defined the concept of tacit knowledge by conceptualising the social and technical requirements that can be used to understand, extract and codify this particular knowledge from a proposed *SecBase* repository system. An attempt has been made to demonstrate a gap between the social and the technical ways of understanding tacit knowledge, and has proposed a way in which the gap could be filled using integrated collaborative technologies. The paper has explained the various dimensions of security risk management that could be impacted by tacit awareness when one reflects on extemporaneous actions. These actions, in a sense *situated* could be analysed by monitoring the collaborative technology streams in the organisations and mapping the knowledge (tacit knowledge) with the *SecBase* repository system. How the *SecBase* system is used could be of importance particularly when monitoring the influence it would have on security risk activities (control and mitigation). As demonstrated, one way of usefully extracting this knowledge is by use of a proposed algorithm that would extract security risk related knowledge embedded deeply in the minds of people, through finding its way into collaborative environments. It is believed that with this understanding, security professionals and other whose interest lies with risk management will be better placed to tap and retain this knowledge within. Future work could involve formulating the aforementioned algorithm to specific cases.

REFERENCES

Baumard, P., (1999) "*Tacit Knowledge in organisations*", London & Thousand Oaks: Sage.

Chambers, C., Dolske, J., Iyer, J., "*TCP/IP Security*" visited 19.07.2005
http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html.

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., (2000) "*From Control to Drift"*, Oxford: Oxford University Press.

Cunha, M. P., Cunha J. V., and Kamoche, K (1999) "*Organisational Improvisation; What When, How and Why* "International Journal of Management Reviews (1:3), , pp 299-341.

Forno, R. and Baklarz R.,(1999) "*The Art of Information Warfare"*: Insights into the knowledge warrior philosophy, Universal Publishers.

Information Systems Audit and Control Association (ISACA) "*Compliance Grid for the ISACA Model Curriculum for IS Audit and Control"* visited 07.07.2006
www.isaca.org/TemplateRedirect.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=21617

Jackson, W., (2006) "*Time to focus on security, not compliance*", Government Computer News, 25 (8): 28, Washington post Newsweek Interactive ISSN 0738-4300.

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.

Ng'ambi, D., (2006) "*Assessing Quality of an Interpretive Educational Technology Research*" WSEAS TRANS on Advances in Engineering Education Issue 2. Vol 3. ISSN:1790-1979.

Nonaka, I., (1994) "*A dynamic theory of organisational knowledge creation*" Organisation Science 5 (1):14-37.

Parker, X., (2001) "*Understanding Risk*" Internal Auditor, 58 (1), Institute of Internal Auditors, ISSN 0020-5745.

Peplowski, K., (1998) "*The Process of Improvisation*" Organisational Science (9:5) pp 560-561.

Polanyi, M., (1966) "*The Tacit Dimension"* London, Routledge and Kegan Paul.

Schultz, E., (2005) "*Security Views*": Computers and Security Journal, Elsevier pp 268.

Siponen , M., T. (2000) "*A Conceptual foundation for organisational Information security awareness*"; Information Management and Computer security journal 8/1 31-41.

Smith, B., Brian, K., Microsoft Security Team (2003) "*Security Kit*": Microsoft Windows Security Resource Kit, Microsoft Press.

Straub, D.,W., and Welke, R.J., (1998) "*Coping with Systems Risk: Security Planning Models for Management Decision Making*": MIS Quarterly, Vol. 22, No. 4,pp. 441-464.

Suchman, L., (1987) "*Plans and Situated Actions: The Problem of Human-Machine Communication"*, Cambridge University Press, Cambridge, UK.

Thompson, M., E. & Von Solms, R., (1997) "*An effective information security awareness program Industry*" Proceedings of WG 11.2 and WG 11.1 of TCl I (IFIP): Information Security for Small Systems to Management of Security Infrastructure.

Von Solms, B., and Von Solms, R., (2005) "*From Information security to…business security*"? Computer and Security Journal, Elsevier, pp 272.

Wagner, R., K., and Sternberg, R., J., (1985) "*Practical intelligence in real world pursuits: The role of tacit knowledg*e"; Journal of personality and Social Psychology. 49 (2):436-458.

Weick, K., (1993b) *"Organisational Redesign as Improvisation,"* in G.P. Huber and H. W. Glick (Eds.), Organisational Change and Redesign, Oxford: Oxford University Press pp 346-379.