A Framework for Security Modeling using Knowledge Engineering

GUSTAVO A. SANTANA TORRELLAS
Instituto Mexicano del Petróleo
Perforación de Pozos
Eje Central Lázaro Cárdenas 152 CP 07330
MÉXICO

Abstract: - Organisational Information Systems – as well as related performance and control systems - were modelled on the same paradigm to enable convergence by ensuring adherence to classical information processes routines built into formal and informal information systems. However, this model is increasingly inadequate in the e-Information Systems era that is often characterised by an increasing pace of radical and unforeseen change in the Organisational environments, Information Systems and underlying Security. The new era of dynamic and discontinuous change requires continual reassessment of information and organisational routines to ensure that decision-making processes, as well as underlying assumptions, keep pace with the dynamically changing Information environments. One such conceptualisation is proposed in this article in the form of a framework for developing Organisational Information Security Model using Knowledge Management. The popular technology-centric interpretations of Information Security and Knowledge Management that have been prevalent in most of the information technology research and trade press are reviewed.

Key-Words: - Information Security, Knowledge Management

1 Introduction

The traditional Organizational Information Security Model is driven by pre-specified plans and goals, aimed to ensure optimization and efficiencies based primarily on building consensus, convergence and compliance must be updated. Organizational Information Systems – as well as related performance and control systems -- were modeled on the same paradigm to enable convergence by ensuring adherence to classical information processes routines built into formal and informal information systems. Such construction of Information Systems and the technology related goals for realizing increased efficiencies was suitable for the era marked by a relatively stable and predictable Information Systems development and Security environment. However, this model is increasingly inadequate in the e-Information Systems era that is often characterized by an increasing pace of radical and unforeseen change in the Information Systems and Security environments. The new era of dynamic and discontinuous change requires continual reassessment of information and organizational routines to ensure that decision-making processes, as well as underlying assumptions, keep strong with the dynamically changing Information Systems and Security environments. The changing Information Systems and Security environment, characterized by dynamically discontinuous change, requires a re-conceptualization of Information Security using a Knowledge Management approach, as they have been understood in information system practice and research. One such conceptualization is proposed in this article in the form of a framework for developing an Organizational Information Security using Knowledge Management. It is anticipated that application of this framework will facilitate development of new Security Models that are better suited to the new Information Systems and Security environment characterized by dynamic, discontinuous and radical changes. The subsequent section discusses the demands imposed by the new Information Systems and Security environments that require rethinking such conceptualizations of Information Security with Knowledge Management and related information technology based systems.

2 Conceptual Framework for Information Systems and Security-based Approach

A variety of conceptual frameworks can be useful in planning and designing Information Systems and Information Security Processes. From our point of view these frameworks help ensure that a plan relates to individual and organisational development and to systemic change. The following frameworks, considered together, provide guidance in planning comprehensive, systemic Security Model innovation using a Knowledge Management approach:

Building a Information Security Knowledge Base. The purpose of this phase is to acquire new Information Security Knowledge and information and to build a conceptual understanding of it.

Observing Models and Examples. The purpose of this phase is to study security cases and examples in order to develop a practical understanding of the research.

Reflecting on Your Security Practice. The purpose of this phase is to analyse your security practice on the basis of new Information Security Knowledge.

Changing Your Security Practice. The purpose of this phase is to translate your new Information Security Knowledge into individual and collaborative plans and actions for organizational and transactional change. Activities might include action research, peer-coaching, support groups, and security empowerment.

Gaining and Sharing Security Expertise. The purpose of this phase is to continue to refine your instructional practice, Information Systems and Security with and from colleagues while also sharing your practical wisdom with your peers.

Sparks and Loucks-Horsley (1989) suggest five models that are useful for accomplishing the goals of security development:

- Individually Guided Development.
- Observation and Assessment.
- Involvement in a Security Development
- Development of Security Improvement Process.
- Training in Information Security.
- Inquiry.

3 Information Security: The Information Processing Paradigm.

The relatively structured and predictable organization of an Information Systems and his Security focus on economies of scale. The evolution of the information-processing paradigm over the last two decades to build intelligence and manage change in Information Systems and Security functions and processes has generally progressed over three phases:

1. Automation: increased efficiency of operations;
2. Rationalisation of procedures: streamlining of procedures and eliminating obvious bottlenecks that are revealed by automation for enhanced efficiency of operations; and,
3. Re-engineering: radical redesign of Information Systems and Security processes that depends upon information technology intensive radical redesign of workflow and work processes.

The information-processing paradigm has been prevalent over all the three phases that have been characterised by technology intensive, optimisation-driven, efficiency-seeking organisational change. The deployment of information technologies in all the three phases was based on a relatively predictable view of products and services as well as contributory organisational and industrial structures. Despite increase in risks and corresponding returns relevant to the three kinds of information technology enabled organisational change; there was little, if any, emphasis on Security Model Innovation – 'rethinking the Information Systems and Security'. Based on the consensus and convergence-oriented view of information systems, the information processing view of Information Security using Knowledge Management is often characterised by benchmarking and transfer of best practices.

The information systems themselves -- not the people -- can become the stable structure of the organisation. The information processing view, evident in scores of definitions of Information Security using Knowledge Management in the trade press, has considered organisational memory of the past as a reliable predictor of the dynamically and discontinuously changing Information Systems and Security environment.

4 General Structure of Information Security with Knowledge Management and Multi-Agent Systems Engineering.

We begin by identifying some of the various types of Information Security Knowledge that administrators need to know:

Conceptual Information Security Knowledge, such as the concept of confidentiality, integrity and availability.

Factual Information Security Knowledge, such as the risk assessment and risk evaluation.

Representational Information Security Knowledge, such as how to draw and use a security policy.

Strategic Information Security Knowledge, such as the ability to recognise the applicability of a concept, such as, confidentiality is conserved when there are no external risks or threats, or that security state is conserved when there are no non-standard attacks.

Meta-cognitive Information Security Knowledge, for example, the awareness of underlying security assumptions, or that an answer should be checked by solving the problem a different way.

Self Information Security Knowledge, such as knowing one's likely sources of mistakes, or knowing that one should be more procedural when solving security problems.

Operational Information Security Knowledge, such as how to take the information security procedures in a safe state.

Procedural Information Security Knowledge, such as when to use a policy schema, or when to specify a co-ordinate actions in order to fix problems, or when to re-adequate a policy framework.

Problem-state Information Security Knowledge, which are the features of a problem used for deciding how to solve it. Examples are: knowing that there are no external attacks in a particular problem, or that there are no risk measures in the problem.

In order to discuss the organisational and structural aspects of Information Security using Knowledge Management, we have found it convenient to broadly classify these types into three general categories. We call these three groups: Conceptual Information Security Knowledge, Operational and Procedural Information Security Knowledge, and Problem-State Information Security Knowledge. In Fig. 1, these three general categories are shown in a representation of how experts store content Information Security Knowledge.

We are developing an agent-based planning and control system for a flexible network security system with multiple policies agents. The input of the system is the general policy model of the network to be protected. The output of the system is the final security's state network. The general flow diagram that indicates the global operation of the system is shown in Figure 1. This flow is mainly divided in two stages: an off-line stage and an on-line stage. The off-line stage performs network security task decomposition. It produces a preliminary security plan that consists of a sequence of security procedures and operations and the precedence relationships among them. The input to this off-line stage is the general policy model of a system that is composed of parts. It then generates a preliminary security assessment plan based on risk analysis and vulnerabilities evaluations about accessibility and network stability. The security assessment operations that make up a preliminary information security plan are task level operations. Currently we have implemented two such operations:

- Security Requirements Assessment
- Threat & Risk Assessment

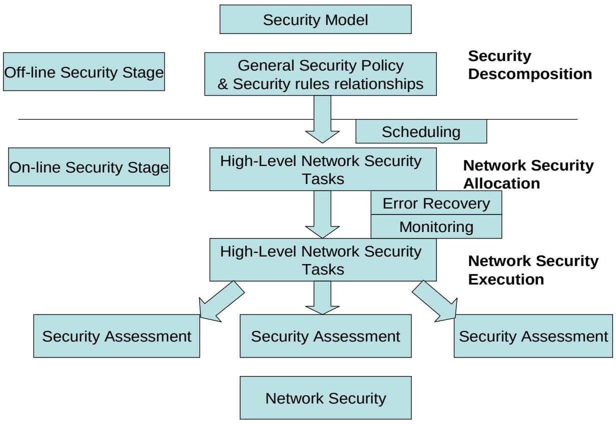

Fig. 1. A representation of an expert's structure of Information Security Knowledge with Multi Agent

This new Information Security using a Knowledge Management approach elements is what some refer to as a schema and often involves problem-state Information Security Knowledge as well. Since the Information Security Knowledge element is conceptual in nature, it becomes replicated (i.e., repeated) in the conceptual bubble. Security Knowledge is one, if not the, principal factor that makes personal, organisational, and societal intelligent behaviour possible. Given the importance of Information Security Knowledge in virtually all aspects of daily and commercial life, two Information Security Knowledge-related aspects are vital for viability and success at any level:

1. Information Security Knowledge assets - the valuable Security Knowledge available to be used or exploited - must be nurtured, preserved, and used to the largest extent possible by both individuals and organisations.
2. Information Security Knowledge-related processes -- to create, build, compile, organise, transform, transfer, pool, apply , and safeguard Information Security Knowledge -- must be carefully and explicitly managed in all areas affected.

In this context, Information Security using Knowledge Management in organisations must be considered from two perspectives with different horizons and purposes (and, require very different expertise) although they to a large extent rely on the same insights in to the organisation's Information Security Knowledge status. These perspectives are:

1. Information Systems and Security Perspective -- which focuses on why, where, and to what extent the organisation must invest in or exploit Information Security Knowledge. Which strategies, products and services, alliances, acquisitions, or divestments should be considered from Information Security Knowledge-related points of view.
2. Information Systems and Security Management Perspective -- which focuses on determining, organising, directing, and monitoring Information Security Knowledge-related activities required to achieve the desired Information Systems and Security strategies and objectives.

5 Information Security using Knowledge Management for Security Model Innovation

As discussed above, in contrast to the information-processing model based on deterministic assumptions about predictability of the future, the sense-making model is more conducive for sustaining competitive advantage in the "world of re-everything". Without such radical innovation, one wouldn't have observed the paradigm shifts in core value propositions served by new Security Models. The Model helps us to discuss:

1. the storage of domain-specific Information Security Knowledge;
2. expert- and novice-like problem-solving behaviour;
3. the hierarchical structure of an expert's Information Security Knowledge store;
4. misconceptions;
5. the effects of goal-free and goal-directed questions; and
6. the meta-communication process.

The system that is structured as a 'core capability' suited to a relatively static Information Systems and Security environment turns into a 'core rigidity' in a discontinuously changing Information Systems and Security environment. In the e-Information Systems and Security era, which is increasingly characterised by faster cycle time, greater competition, and lesser stability, certainty and predictability, any kind of consensus cannot keep pace with the dynamically discontinuous changes in the Information Systems and Security environment. With its key emphasis on the obedience of rules embedded in 'best practices' and 'benchmarks' at the cost of correction of errors, the information-processing model of Information Security Knowledge management limits creation of new organisational Information Security Knowledge and impedes renewal of existing organisational Information Security Knowledge. Most of the innovative Security Models didn't evolve from the best practices or benchmarks of the organisations of yesterday that they displaced, but from radical re-conceptualisation of the nature of the Information Systems and Security. These paradigm shifts are also increasingly expected to challenge the traditional concepts of organisation and industry with the emergence of Information Systems and Security ecosystems, virtual communities of practice.

6 An Implementation for Security Assessments Incremental Planning.

Information Security using Knowledge Management technologies based upon the information-processing model are limited in the capabilities for creation of new Information Security Knowledge or renewal of existing Information Security Knowledge.

As the security assessment agents share the same General Security Policy, collisions among these security assessment agents are possible. To avoid collisions between the network entities as well as between the network entities and the security environment, we have developed an agent based collision avoidance system. The system is based on the concept of *Security Assessment Incremental Procedure* (SAIP). The computation of these steps is coordinated by the Security Assessment Planning Agent and is performed in near real-time during the network security execution. This allows us to produce collision free security state execution, even when the security policies of the network entities are not known in advance. We have developed a distributed Autonomy and agent pro-activeness planning system in which each of the security assessment agents computes its incremental security task.
The Security Assessment Planning Agent assigns a priority to each of the security assessment agents to compute the next security assessment incremental task in the order that has been determined previously. The priority management is both dynamic and

proactive. It is dynamic since the priority is calculated on the fly at each configuration along the autonomy and agent pro-activeness. It is proactive because it takes into account the System Security State at each time instant. The following factors are considered to compute the priority for each security assessment:

- *Network security sequences*.
- *Trust level between the security assessment and its goal configuration*. The closer to the goal configuration the autonomy and agent pro-activeness is, the higher its assigned priority.
- *Trust level between security assessment and autonomy/agent pro-activeness*. A higher priority will be assigned to the security assessment that is closer to the security statements that are about to be assembled.
- *Security assessment priority history*. In order to achieve load balancing for security assessment agents, the security assessment, which has been utilized frequently, will be assigned a lower priority.
- *Security assessment failure*. If a security assessment breaks down during execution, it will be assigned a high priority so that the following Security Assessment planning will first consider the broken security assessment and plan accordingly.

Once the priority of each security assessment is determined the next security assessment incremental security task of the autonomy and agent pro-activeness will be computed. The calculation of security assessment incremental security task of the security assessment agents is based on an artificial potential field technique [6]. This technique uses artificial potential (forces) to model the Security Assessment-planning problem. There are two kinds of potentials: attractive potential generated by the goal configurations of autonomy and agent pro-activeness agents and repulsive potentials generated by misconfigurations. These two potentials encourage a security assessment to move towards its goal configuration and keep it from moving towards the misconfigurations. Time is considered as another independent variable to determine the security task of the autonomy and pro-activeness agents. The following information is needed in order to calculate the security assessment: Current and goal configuration of the security assessment, Connection status, models of trust domains, security assessment agents, inter-domain configurations, transactions, and, security policies parts that have been assembled.

This approach can be treated as a search problem, which aims to find a shortest collision-free Security Assessment. We have developed a heuristic search approach to generating collision-free security state policies. For each security assessment at its current configuration, all feasible states are generated. Each state is represented by the following parameters: Trust level between the current configuration and the goal configuration of the security assessment The states of the all system components. When both, the priority and the best security assessment task, have been calculated at each time instant, the complete security tasks of the security assessment agents can be obtained. Until information systems embedded in technology become capable of anticipating change and changing their basic assumptions (heuristics) accordingly, we would need to rely upon humans for performing the increasingly relevant function of self-adaptation and Information Security Knowledge creation. The human aspects of Information Security Knowledge creation and Information Security Knowledge renewal that are difficult -- if not impossible -- to replace by Information Security Knowledge management technologies are listed below. Imagination and creativity latent in human minds Untapped tacit dimensions of Information Security Knowledge creation.

4 Conclusion

Information Security using Knowledge Management and Multi-Agent Systems activities are adding value to organizations by enhancing Information Systems and Security innovation and innovativeness. Some management experts have discussed selected aspects of the proposed sense making model of Information Security Knowledge management in terms of the shift from the traditional emphasis on transaction processing, integrated logistics, and work flows to systems that support competencies for communication building, people networks, trust-building and on-the-job Information Systems and Security. Many such critical success factors for Information Security Knowledge management require a richer understanding of human behavior in terms of their perceptions about living, Information Systems and Security and working in technology- mediated and cyberspace-based environments. The need for better understanding of human factors underpinning performance of Information Security Knowledge Management technologies is also supported by our observation of informal ‘Information Security

Knowledge Sharing' virtual communities of practice affiliated with various Net-based Information Systems and Security's and related innovative Security Models. It is suggested that the critical success factors of the proposed model of Information Security Knowledge Management for Information Systems and Security innovation are supported by a redefinition of 'security control' as it is relates to the new living, and working environments afforded by emerging Security Models. Hence, Security Model Innovation needs to be informed by the proposed model of Information Security using Knowledge Management that is based upon synergy of the information-processing capacity of information technologies and sense-making capabilities of humans. Information Security using Knowledge management is one set of approaches to doing this, which seems to meet with some success. We have explored here for the first time the impacts of Information Security Knowledge management on Information Systems and Security innovation processes, but our investigation has only scratched the surface. Further research still needs to be done on the specifics of the innovation/Information Security Knowledge management interaction, especially around factors of causality, differences among various types of innovation and their Information Security Knowledge needs, and industry- and company-level variations in implementation and diffusion patterns. While there may never be an explicit Information Security Knowledge-to-innovation translation mechanism, we will continue to explore how to support growth and innovation efforts through more effective Information Security Knowledge management.

References:

[1] Alon Y. Levy et al., Query answering algorithms for information agents, *AAAI'96 Proceedings*, 1996.

[2] Gustavo Santana et al., Methodological **Network Security Process Modelling: Integrating Security Requirements with Multi-Agent System Engineering**, *NPDC2002 IASTED Inetrnational Conference Proceedings*, Tsukuba, Oct. 2002.

[3] M. Abadi, M. Burrows, B. Lampson, and G. D. Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, September 1993.

[4] A. W. Appel and E. W. Felten. Proof-carrying authentication. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, Singapore, November 1999.

[5] FIPA - "FIPA'97 Specification Foundation for Intelligent Physical Agents" – drogo.cselt.stet.it.fipa – 0ctober 1997

[6] C. M. Ellison. Establishing identity without certification authorities. In *Proceedings of the 6th USENIX Security Symposium*, San Jose, July 1996