December 2006

Deep Structures of Information Systems Security

Manoj Thomas
Virginia Commonwealth University

Gurpreet Dhillon
Virginia Commonwealth University

Deep Structures of Information Systems Security

Manoj A Thomas
Virginia Commonwealth University
mthomas@vcu.edu

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

ABSTRACT

Companies tend to adopt security approaches that align with some subset of the four categories of IS security techniques - checklists, risk analysis, formal methods and soft modeling. To develop a structure of secure IS that upholds confidentiality, integrity and availability of information there remains a need for an integral security model that incorporates the benefits of other security designs outside the chosen ones. Organizations demand security models that cater to their unique operational characteristics. The paper uses the deep-structure model of Wand and Weber (1990) to help reveal the deep structure characteristics of IS security using three models - representational model identifies subsystems within an organization; state-tracking model ensures security changes trace real world security system changes; and decomposition model defines specific external events that are stimuli to changes on internal events. A conceptual security model is presented that manifests the meaning of dynamic, custom-fit and flexible IS security structure which also incorporates features from checklists, risk analysis, soft modeling and formal methods.

Keywords

Information Systems Security, Deep Structures

INTRODUCTION

Just as deep structure of an information system comprises those properties that manifest the meaning of real-world systems that the information system is intended to model, the deep structure of IS security should comprise those properties that manifest as the meaning of security that a secure IS model is intended to model. In an organizational setting where growth is accompanied by normal operational disruptions and confusions, the only means to accomplish a secure IS that upholds confidentiality, integrity and availability (Bishop, 2002) is to develop a structure of IS security that is adaptive and flexible to reorganize itself with the changing environment of the organization and the behavior of the actors involved. In some sense, this implies that an effective IS security model is one that is dynamic, predictive and preventive to counter any internal or external security threats to the organization.

To accomplish these goals, this paper describes three interconnected models that describe IS security deep-structure. The deep-structure properties are in alignment with the three models proposed by Wand and Weber (1990) and seeks to facilitate the analysis, design and implementation of a faithful IS security design model. This paper is motivated by the premise that a deep rooted analysis of IS security will help to reveal the deep-structure characteristics of IS security in a way that it models real expectations of information security. Furthermore, a concrete study will also help to naturally identify the forces that hold the components together and influence the holistic behavior of the security model under varying internal and external events. A conceptual model of this form will help to formulate an IS security design that will faithfully track the security events in the real world and propagate pertinent and requisite changes to all coupled components which in turn will most effectively ensure confidentiality, integrity and availability of information to the users. The model proposed in this paper is based on defining Information Systems security as the protection of information resources of a firm, where such protection could be through technical means and by establishing adequate procedures, management controls and managing the behavior of people (Dhillon and Torkzadeh, 2006) and focuses only on the *deep-structure* of IS security.

OVERVIEW OF IS SECURITY DESIGN MODELS

Numerous attempts have been made to grapple with the challenges of establishing a secure information system. Research in the area of IS security can be classified into one of four categories: checklists, risk analysis, formal methods and soft modeling techniques (Dhillon and Torkzadeh, 2006; Siponen, 2001; Backhouse and Dhillon, 1996).

Checklists provide a security evaluation guide without addressing the key task of understanding the substantive questions of security in the given organizational context. Risk analysis portray the correspondence between risk and vulnerability and helps IS managers to justify the cost of IS security implementation and control. Critics of risk analysis methods question the use of probability theory to assess security risks. Formal methods, on the other hand, are discrete event-oriented approaches whose origin can be traced to application in military environment. They derive solutions by abstraction of the problem and the solution space (Baskerville, 1993). The Bell La Pedula Model and the Trusted Computer Systems Evaluation Criteria are examples of formal methods of IS security design. The highly structured approach makes them limited in long term usefulness. Soft modeling design methods that rely on social theories to study security issues have gained significant attention in recent years. They help to attain a holistic view of the problem domain that is lacking in all prior design methods that have been proposed. Although soft modeling methods help to recognize the importance of a changing organizational context, including with the role of human and social attributes, they are limited in prescriptive components and orient towards offering complex philosophical and sociological explanation to security problems (Dhillon and Backhouse, 2001).

All of the above security modeling techniques offer unique features that are vital in establishing an impregnable security solution. However, none of the methods on their own have guaranteed a fully anchored Information System security as evidenced by the lack of large scale adoption of any one of the design techniques in the practitioner world. The validation of the argument is an easy task. There is little doubt that IS security implemented as a set of items crossed out from a checklist is any more effective than using risk analysis that weighs security costs to expected benefits. Neither is the use of formal controls to derive effective solutions by abstraction of the problem and solution space (Baskerville, 1993) more effective than soft modeling techniques that recognize the importance of changing organizational context, human and social attributes. The underlying problem is not really a lack of rigidity in each of the propositions, but rather a completeness that fail to include the benefits of other security design models besides those offered from within themselves.

The classic definition of IS security is conceived on the notion of Confidentiality, Integrity and Availability (CIA) of data (Bishop, 2002). *Confidentiality* refers to limiting data access to authorized users through authentication methods and controls. *Integrity* implies the ability to preserve trustworthiness of the information resources by ensuring that changes are not made inappropriately. Equally critical is *Availability*, which refers to the fact that the information sources actually remain available, since unavailability is as good as having no information at all. Although CIA is a widely used benchmark for evaluating information systems security (Magnusson and Yngstrom, 2004), it is highly restrictive and the golden goose for successfully managing information security is to also inculcate principles of Responsibility, Integrity, Trust and Ethicality (RITE) into organizational minds. *Responsibility* insures duty (or obligation) to the sphere of activities that surround work practices and events that defines an organization's sense of security. *Integrity* is the requirement of membership that upholds steadfast adherence to ethical code of conduct and *Trust* can be defined as the cohesive element that binds work force to institutions especially when organizations rely on information assurance to effectively sustain and strengthen itself. *Ethicality* embodies what is right and wrong in the conduct of endorsing information security. It refers to the informal norms and behaviors which are not explicitly stated as company rules that can be applied to all formalized procedures. While CIA is mostly operationalized through technical aptitude, RITE principles evoke a strong social imprint. Gladly, in the communal space of IS security research, the dire necessity of CIA and the invisible forces of RITE have not gone unnoticed. The outcome has been a renewed call for inquiry into IS security research that aims to combine CIA with the principles of RITE (Dhillon and Backhouse, 2000). The importance of this problem has been vocalized loudly in the hope that there is some means by which organizations will be sufficiently prepared with the right IS security model – a model that is suited to the individual characteristics of the environmental dynamics in which they operate.

Companies tend to adopt security approaches that are more or less in alignment with any one of the four prominent representations of IS security design models. Organizational settings that focus on using social theories in understanding security issues have inherently higher benefits attained by gaining a holistic view of the problem domain. However, they lack in prescriptive components and tend to focus on explanations that are enshrouded in complex philosophical and sociological bases (Dhillon and Backhouse, 2000) Information Systems security will forever remain inadequate under any circumstances that fail to encapsulate the sociological, technical, well-defined internal events and specific external components that shape the functioning of an organization. The reality is that, even today it is not uncommon to come across companies that seek to

accomplish IS security through a set of checklist items and some related hardware and software installation. Irrespective of whether such seemingly uninformed IS security solutions is due to the lack of attention, unawareness or optimistic biases, there remains a strong need to develop a security model that manifests the meaning of what constitutes dynamic, flexible and predictive IS security design model.

One plausible way to realize this manifestation is homologous to the way marine biologists study unfamiliar deep sea territories through deep sea diving expeditions. Just as a diver would conduct observational investigation of the depths of the ocean and assemble the outcome of the observations on return to the surface, the researcher can attempt to identify the deep structures of organizational IS security, where observations of the subcomponents can be harmonized as an interpretation of what constitutes real IS security. Decomposing the aggregate into its sub-components, analyzing the components at a granular level and weaving the relationships that unify the components at an organizational level will enable the development of a precision fabricated IS security design model that is consistent with the social expectations and in concordance with the internal and external events in which the organization ultimately functions.

Wand and Weber (1990) uses the deep-structure model to characterize Information Systems in a similar manner. The concept of deep structure is not really new to the field of IS. Deep-structure was originally proposed by Noam Chomsky as a means to explain the notion of rules and generative grammar used in linguistics to explain the process of organizing (Truex and Baskerville, 1998). This notion, borrowed from linguistics, has been used to characterize the process of organizing the surface, deep and physical structure of information systems. Leifer (1994) uses deep-structures to elicit knowledge that escapes systems designers by analyzing knowledge types and task characteristics. Wand and Weber (1990) adopts an approach where they regard *surface-structure* as the interface between the information system and its users and organizational environment. The *deep-structure* captures the essence of the real world systems that the information system is intended to model and *physical-structure* manifest the technology used to implement the system. Furthermore, by adorning *deep-structure* as the window to the soul, they seek to reveal the behavior and the fabric of interaction in what constitutes a 'good' information system (Wand and Weber, 1990). They define the properties of *deep-structure* by using three models – the representational model, the state-tracking model and the decomposition model.

The same deep-structure approach can be successfully applied to capture the essence of what truly characterizes IS security. A deep analysis of the components of IS security can also be realized by using the representational, state-tracking and decomposition models proposed by Wand and Weber. The models can be used to describe the ontological constructs and the grammar that manifest real world security system. The relationships between the models will describe how changes in one invoke correlative changes in other sub-components. In many ways, this is akin to a web of interactions where concepts from the four individual IS security design methods is solicited to create a comprehensive bubble or an *integral completeness*, that is currently lacking in each of individual IS security models. Naturally, in this web of interaction, the relationships between the models play a vital role. Failure to address the role of relationships is arguably the root cause of deficiencies and inaptitude in the IS security models.

THE FRAMEWORK

Chomsky (1967) intended to use the concept of deep structures for evaluating spoken languages and related grammar. Application of deep structure principles for the analysis of Information Systems properties evolved from recognizing the problem associated with capturing the true meaning of information systems (Wand and Weber, 1990; Leifer, 1994). The framework used in this paper borrows heavily from the formal deep-structure model (consisting of the representational model, the state-tracking model and the decomposition model) proposed by Wand and Weber (1990). Wand and Weber use representational model to generate scripts that describe the structure and behavior of a real-world system. The state-tracking model engages in helping reveal whether the information system truly tracks the real-world system that it is intended to model. The model accomplishes this using four necessary and sufficient conditions – mapping requirement, tracking requirement, reporting requirement and sequencing requirement. Finally the decomposition model is used by Wand and Weber to define the static and dynamic nature of events (both internal and external) and their state (stable or unstable) of existence. The deep-structure framework applied to IS security can be conceptually mapped as shown in figure 1.

Representational Model:

The deep structure interpretation of real world IS security consists of describing the elements and subsystems that are sufficient and necessary to establish a secure information system. The ontological constructs in the representational model

enable us to identify the properties and requirements of all components that facilitate the development of a high level security mechanism in a way that satisfies the end user and the organization while also being effective and efficient in the given organizational context (Markotten, 2000). The ontological formalisms for describing the representational model of information security can be developed by extending the construct proposed by Bunge (1977, 1979). Developing these constructs for the security model is an ongoing research issue. The representation model is not the actual security software or hardware, but an ontological formalism that defines the structure and behavior of ideal real world IS security system. The formalism can be cast into implementations of security techniques (such as cryptographic methods, security monitoring devices) using the *physical structure.*

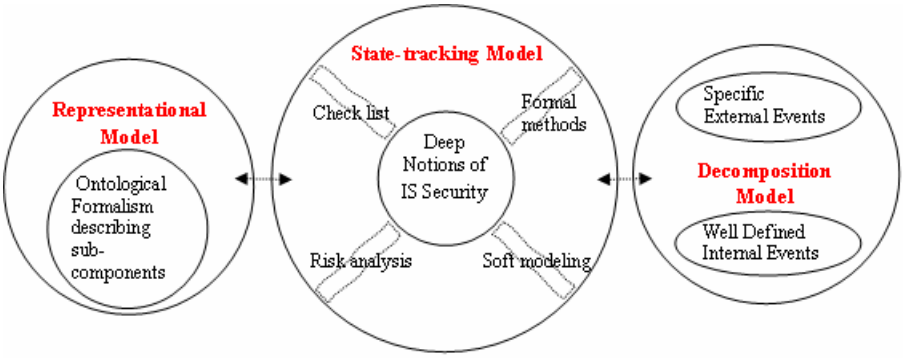

Figure 1. The Conceptual map of IS security deep structures

State-tracking Model:

The state-tracking model actively seeks to follow the footprints of the real world IS security that it intends to model. Wand and Weber specifies four necessary and sufficient conditions for an information system to faithfully track the real world system. These conditions ensure completeness of the IS security model and help to evaluate the congruence of the model to the real world. Organizations thrive by seeking equilibrium with their environment. Correspondingly as the environment changes and evolves, the consequences also affect the organizations. This is similar to what biologists would refer to as *co-evolution* (Wheatley, 1999). Modeling an IS security system that is heavily structured and rigid will severely constrain the IS security from adapting to fluctuations within the organization and changes in the environment. Higher levels of resiliency and coherence to changes in the real world are requirements in a security model if organizations are to feel unthreatened while operating in the midst of an environment that is unpredictable and susceptible to constant flux. No single IS security model adequately addresses the effect of changing environmental states on the organization and vice versa. An effective IS security model should incorporate features from checklists, risk analysis, soft modeling and formal methods to ensure checks and balances that address such changes. This may come across as a 'porridge of security being' and is precisely what the state-tracking model seeks to handle. The goal of the state-tracking model is to track the changes and enable organizations to undertake an agile and responsive security policy development strategy.

Four necessary conditions hold for the state-tracking model. These conditions are closely related but amended versions of those proposed by Wand and Weber.

Requirement 1: A one-to-many mapping must exist from the set of real-world security system states into the set of IS security states.

This corresponds to the *mapping requirement* that when satisfied ensures that at least one IS security state exists for every real-world security state.

Requirement 2: When the real-world security changes state, the IS security must be able to change from a state that corresponds to the initial real-world security state to a state that corresponds to the subsequent real-world security state.

This is the *tracking requirement* to ensure that IS security model responds to state changes in a manner corresponding to the security incident changes in the real-world system.

Requirement 3: If an external event occurs in the real-world security system, an external (input) event that is a faithful representation of the real-world external event must occur in the IS security model.

This *reporting requirement* warrants that any IS security external event is an accurate and complete representation of the real-world security external system security event. Although the real world security event may not necessarily affect the organization, the IS security design should be aware that this external event occurs in the real world.

Requirement 4: The order in which external events occur in the IS security model must be the same as the order in which external events represented by these IS security system external events occur in the real world system.

This is the *sequencing* requirement to ensure that the IS security model does not loose track of the real world IS security states because external events are not occurring in the IS security model in the correct order.

The requirements are not intended to enforce control, but enable dynamic connectedness that match the features from checklists, risk analysis, formal methods and soft modeling.

Decomposition Model:

The decomposition model breaks down IS security structure into architectural sub-systems that allow a fine-grained view of individual components and their security requirements. The decomposition model defines all specified external events and well-defined internal events. The reality is that, there exists a strong interaction between the organization and the environment. Describing the direct and indirect influence of the internal and external events and the propagation of the effects to all other interconnected sub-components is the goal of the decomposition model. This opens the potential for predictability and planning in the IS security model in a way that helps to attain *the integral completeness* in the conceptual design.

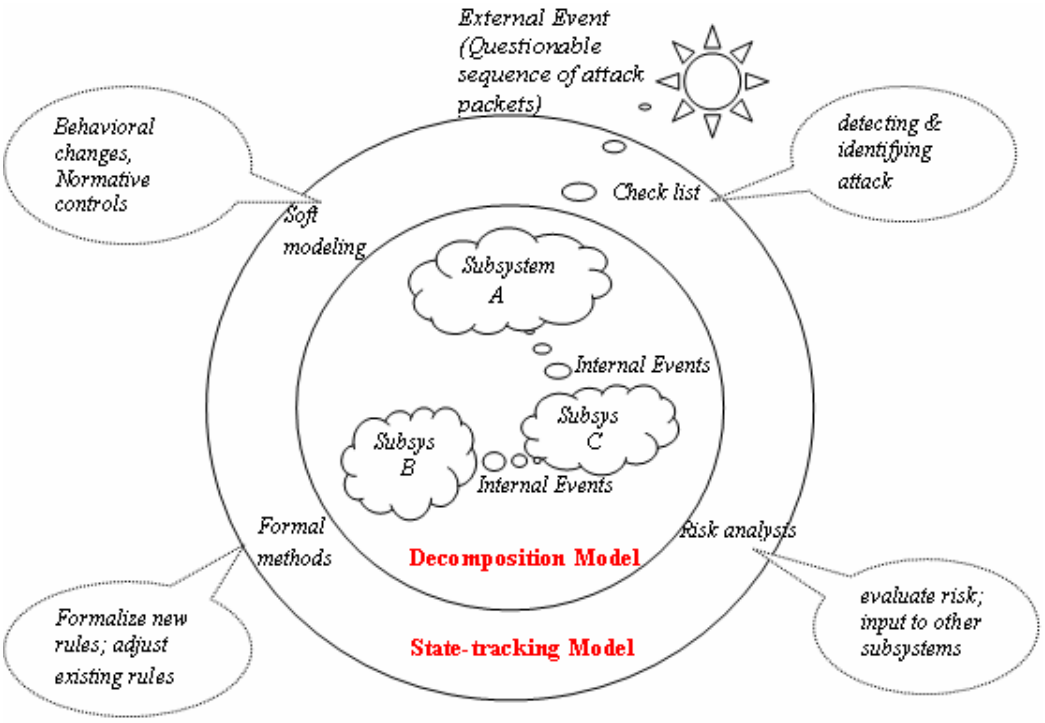

Figure 2. Applying the Deep Structure Model of IS Security.

In order to demonstrate the nature of the model, consider an external event, such as a questionable sequence of packets identified by a well known attack pattern logged at the intrusion detection system of the organization. This external event can act as a stimulus to one or more of the sub-systems of the organization. The sequence of packets in question evokes a response, an internal event, from the security gatekeeper of the affected subsystems. The gatekeeper, in turn could alert the caretakers of other critical functional units (or subsystems) of the company that are vulnerable to the threat. This reflects the indirect effect of changes in one subsystem on other subsystems. The sequence of events, starting with the external event (a plausible attack) from which new information is spawned (detecting the attack source), followed by generation of new meaning (identifying the attack source) and subsequently conveying warning messages to other functional units, illustrates the interaction and reflective conversation among different subsystems of the organization. The set of interactions resulting from the external and internal events can be decomposed and represented as shown in figure 2.

The importance of interrelationships between the architectural spaces that form the overall system cannot be undermined. The internal events may either be well or poorly defined. Well defined internal events are predicable state changes of subsystems based on specific external events. Poorly defined internal events are outcomes of unexpected subsystem state changes due to unspecified external events. Although unspecific external events can stir things up and roil the pot, causing service disruption and confusion, they create new information for the state tracking model. This new information is the very substance that draws together the features from checklists, risk analysis, formal methods and soft modeling, creating a communal space of interacting influences and invisible forces allowing continuous growth and change to the security preparedness model of the organization. While checklists and risk analysis help prevention, prediction, risk assessment and monitoring, formal methods assist with planning and establishing rules for adequate checks and balances. Soft modeling enables internal monitoring, generates security literacy among employees, places normative controls, allows information monitoring and lays down a strong accountability and responsibility structure (Dhillon, 2001).

AN EXAMPLE

The description of a conceptual model can sound teasing and enticing in many ways until it is validated or falsified otherwise. Although a real world validation is the preferred choice for any research, analyzing the application of the conceptual model as it applies to a real world scenario can be equally invigorating. For the sake of clarifying the use of the conceptual model (in addition to the example in the previous section), consider the following email notification sent by the security manager at an organization with approximately 13000 employees, a week prior to the date mentioned.

> *An email worm known as BlackWorm/Nyxem/Blackmal/Blueworm/Grew is scheduled to delete (actually overwrite with a small text message) certain file types on Feb 3, 2006. Microsoft sees this threat as low but it's always good to be aware. Make sure your virus definitions are up to date.*

Although the intent of the email message is to warn users about an impeding attack in the future, the message is vague, the events are poorly defined and specified preventive steps lack any purpose. Even the name of the impending virus has no real meaning to a normal computer user. Checklists and risk analysis provide no additional clarity to the message related to the probable incident in the future. Dealing with an unspecified external event of this nature is a hard security situation at hand for any organization. Once the external environment has gained adequate awareness of the incident, which in most cases is long after the incident has occurred, useful knowledge is made publicly available from security response teams like CERT/CC or CIS (see references 6,8,16 and 18). This new information is reactive in nature but can strengthen existing checklists and risk analysis approaches to protect against future attacks of similar nature. It is also important to note that organizations that are the first victims are faced with a crisis and whatever adverse consequences the problem portends, are therefore inescapable after the threshold of response timeliness has passed. Unspecified external events, however, need not necessarily leave an organization in the dark. The email warning in this case serves value through the use of formal methods and soft modeling. Internal events triggered from the external stimuli include adapting existing rules as precautions or adding new formal rules to proactively curtail the effects when (or if) the external event is incident to the overall system. In addition to use of formal methods, soft modeling can mitigate risk through immediate internal controls and reasonably assure that control objectives are being met. Soft modeling can also impose external controls to audit the requisite behavioral changes needed to cope with the formal rules and define the role of responsibility structures. Combining features from the four models manifest into reflections of expected agility and flexibility needed in a real world Information Security model.

CONCLUSION

In an area of IS research severely limited by the lack of a strong IS Security theory that is coercive and does not disregard the importance of the information systems, its users and the organizational environment, it is imperative that an ontological approach focused on gaining a deep understanding of organizational security would be the first step in the right direction. Since it is impossible to know everything there is to know about security, and because it is impossible to predict the next critical security incident, or where personal motivations condense into dubious security concerns, a devotion to understanding patterns, rules, direction and internal rhythm of organizations will offer an imagery of a singular reality that can be captured in a cohesive security model. Identifying the deep structure properties of IS security will therefore help to better understand the underlying phenomena that characterize real IS security expectation.

Motivation for this research stems from the potential to elucidate deep structures of IS security in a way that it models real expectations of information security by following a treatment similar to that established by Wand and Webber (1990) in characterizing the deep structure of information systems. The model presented in the paper provides a conceptual view of an IS security design model based on this exposition. Deep structure offers a rich understanding of IS security manifestations by combining all the aspects of real world IS security that will help to attain higher levels of effectiveness in securing the valuable resources of an organization. Conceptualizing the properties of IS security model by applying the three models of deep structure suggests an organizational security design that uses surface information, interprets deep structure consequences and applies the right technical solutions. The conceptual model presented in this paper is flexible to accommodate the changes that an organization go through on a regular basis and provide a means to preserve security of resources without being wedged into one of the many rigid security models that is unsuited to meet the challenges of fast changing internal and external security threats. By drawing parallels to the linguistics of Information Systems deep structure, the model allows deep structure information to arise automatically in all applied IS security situations.

Finally, it is pertinent to point out that deep structure analysis of information systems proposed by Wand and Weber has its own set of limitations. It falls short in its modeling power primarily due to the lack of a well defined ontology that allows "semantic modeling" of the domain of discourse (Wand and Weber, 1990). IS security, on the other hand, is a specialized topic well suited for a deep structure analysis mainly due to two important reasons. 1) the mélange of specific external events and consequent internal events are well studied, documented and made public by numerous security response teams such as CERT/CC, CIS, CSRC and NSA (see references 6,8,16 and 18) and 2) the need for developing well defined taxonomies that classify attacks, incidents and vulnerabilities has been recognized and commercial and federal bodies have joined hands in addressing this issue (John Howard, 1997). Continuing research will focus on developing ontological constructs that can describe the three models within the deep structure and develop vocabularies that depict the four requirements of the state-tracking model as well as the event states of the decomposition model.

REFERENCES

1. Backhouse, J. and Dhillon, G. (1996) Structure of responsibilities and security of information systems, *European Journal of Information Systems*, 5(1), 2-10.
2. Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development, *ACM Computing Surveys*, Vol.25, No.4.
3. Bishop, M. (2002) Computer Security: Art and Science, Addison-Wesley Professional, 1st Edition.
4. Bunge, M. (1977) Ontology I: The Furniture of the world, D. Reidel Publishing company.
5. Bungee, M. (1979) Ontology II: A World of Systems, D. Reidel Publishing company.
6. Carnegie Mellon Software Engineering Institute CERT Coordination Center (accessed 15th Jan, 2006) http://www.cert.org/
7. Chomsky, N. (1967) Synthese, Springer publications, Volume 17, Number 1.
8. Computer Security Resource Center (accessed 15th Jan, 2006) http://csrc.nist.gov/pcig/cig.html/
9. Dhillon, G. (2001) Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns, *Computers & Security*, Vol.20, No.2, 165-172.
10. Dhillon, G. and Torkzadeh, G. (2006 forthcoming) Value-focused assessment of information systems security in organizations, *Information Systems Journal.*
11. Dhillon, G. and Backhouse, J. (2000) Technical Opinion: Information Systems Security Management in the New Millenium, *Communications of the ACM*, vol.43, No.7.

12. Howard, J., (1997) An Analysis of Security Incidents on the internet, Unpublished Thesis, Dept. of Engineering and Public Policy, Carnegie Mellon University.
13. Leifer, R., Lee, S., and Durgee, J. (1994) Deep Structures: Real information requirements determination, *Information and Management*, 27, 275-285.
14. Magnusson, C., and Yngstrom, L., (2004) Method for insuring IT risks, Proceedings of the 37th Hawaii International Conference on System Sciences.
15. Markotten, D., (2002) User-centered Security Engineering, *Proceedings of the 4th EurOpen/Usenix Conference*, Helsinki, Finland.
16. National Security Agency (accessed 15th Jan, 2006) http://www.nsa.gov/snac/
17. Siponen, M.T., (2001) An analysis of the recent IS security development approaches: descriptive and prescriptive implications, Information Security Management: global challenges in the new millennium, Eds. G. Dhillon, Hershey, Idea Group Publishing.
18. The Center for Internet Security (accessed 15th Jan, 2006) http://www.cisecurity.org/
19. Truex, D.P. and Baskerville, R. (1998) Deep structure or emergence theory: contrasting theoretical foundations for information systems development, *Information Systems Journal*, vol.8,2,99-118.
20. Wand, Y. and Weber, R. (1990) Towards a theory of The Deep Structure of Information Systems. *International Conference on Information Systems*, pp.61-71.
21. Wand, Y. and Weber, R. (1990) An ontological model of an Information System, *IEEE transactions on Software Engineering*, Vol 16, Number 11, pp.1282-1292.
22. Wheatley, M. Leadership and the New Science, Barrett-Koehler Publishers, 1999.