Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2010 Proceedings

European Conference on Information Systems (ECIS)

2010

A Holistic Approach for Enriching Information Security Analysis and Security Policy Formation

Jeffrey, May
James Madison University, mayjl@jmu.edu

Gaurpreet Dhillon
Virginia Commonwealth University, gdhillon@vcu.edu

A HOLISTIC APPROACH FOR ENRICHING INFORMATION SECURITY ANALYSIS AND SECURITY POLICY FORMATION

Journal:	*18th European Conference on Information Systems*
Manuscript ID:	ECIS2010-0178
Submission Type:	Research Paper
Keyword:	IS security, IS policy, Organizational culture, Socio-technical approach

A HOLISTIC APPROACH FOR ENRICHING INFORMATION SECURITY ANALYSIS AND SECURITY POLICY FORMATION

May, Jeffrey, James Madison University, Harrisonburg, Virginia, USA, 22807, mayjl@jmu.edu

Dhillon, Gurpreet , Virginia Commonwealth University, Richmond, Virginia, USA, 23284, gdhillon@vcu.edu

Abstract

Past literature has indicated the need for addressing information security from both the social and technical perspective. However, previous research has lacked in providing any clear direction for how these two perspectives can be brought together in a coherent or holistic manner to analyze information security in an organization. Thus, this paper develops a conceptual framework for identifying, bringing together, and interpreting the deep-rooted social and technical issues that pertain to information systems security. The framework is grounded in semiotics and is validated by the analysis of a specific case study. Findings in this research indicate that the social and technical elements of security can be brought together in a holistic manner via six layers of abstraction where each layer addresses deep-rooted issues that pertain to information security. The output of each layer is then used to inform other layers in a collaborative manner creating a final product that contains elements for enriching security analysis and enhancing security policy formation.

Keywords: Information Security, Semiotics, Security Analysis, Security Policy

1 INTRODUCTION AND CONCEPTUAL BASIS

For an organization to secure its information assets, a plethora of both social and technical issues must be considered. For example, Rainer *et al.* (2007) provides a detailed list of 25 important issues for the purposes of maintaining information security. These issues that include: confidentiality, integrity of data, access control, availability of data, and physical security, are more technical in nature and have been the main focus of researchers since the advent of information security research (Anderson, 2007). However, more recently, various social issues have become important areas of focus for ensuring information security. For example, Backhouse and Dhillon (1996) describe the importance of responsibility structures being established. Stanton *et al.* (2005) describe the importance of positive security leadership and clear designation of user roles and responsibilities to create a more positive security environment for end-users. Herath and Rao (2009) describe the impact that intrinsic and extrinsic motivators may have on end-user compliance. And Dhillon and Torkzadeh (2006) present an array of nine fundamental objectives for maximizing information security that include issues such as: maintaining an ethical environment, maximizing organizational integrity, privacy, maintaining the integrity of business processes, and developing sound management development practices.

No doubt, the literature has begun to recognize the need for incorporating both social and technical issues into the analysis and design of securing information systems and for creating sound organizational security policies. Kritzinger and Smith (2008) contend that technical information security issues should not overshadow the non-technical information security issues. Theoharidou *et al*. (2005) contend that information security is emerging into a new paradigm that requires a multi-disciplinary approach. And Dlamini *et al.* (2009) concludes that new research efforts are required that minimize the gaps between social and technical issues. However, as we move forward to address new challenges that result from considering social factors, it is also critical that we continue to improve upon our technology. In other words, to analyze and design secure information systems and to create sound organizational security policies, a balance of the two perspectives is required.

However, as the number of security issues increases so too does the complexity of designing and maintaining secure information systems. Thus, a number of researchers have called for simplifying the conception of information security via the development of holistic models and frameworks (Eloff and Eloff, 2003). For example, Anderson (2007) presents a holistic model for risk management that attempts to merge the roles of executives and security practitioners in organizations. Zucatto (2007) describes a holistic framework that attempts to organize processes that provide a smooth interaction between organizational business process, its technological security issues, and social driven security management for electronic commerce. And Kritzinger and Smith (2008) have conceptualized a holistic model (ISRA Model) that attempts to enhance information security awareness among employees. However, these models are either too focused on a particular industry segment or have not been grounded via proper theoretical investigations.

Thus, this research will provide a holistic and general framework for conceiving information system security. The framework developed in this research is grounded by the theory of semiotics. Barley (1983) comments that semiotics offers an approach for researching and analyzing the deep-rooted systems of meaning that lie beneath organizational cultures. Andersen (1992) believes that semiotics provides a theoretical tool to analyze both "soft" areas like interface design and user friendliness along with investigating the technical construction of computer systems. And Braf (2001) states that semiotics provides an adequate theory for developing conceptual frameworks to better understand the deep-rooted technical and human issues that pertain to information flow amongst complex systems. Clearly, information security involves a plethora of complex issues that involve both technical and human factors. Therefore we argue that developing an understanding of IS security via the use of semiotics would serve

to uncover the surface-level and deep-rooted issues that may often times be overlooked by security experts but are critical to ensuring secure information systems.

Several researchers have taken a semiotics approach to analyzing various issues related to information systems. For example, Nadin (1997) introduced using the semiotic paradigm for designing information systems and argued that regardless of whether or not system designers know it, they are in fact using various concepts of semiotics when designing user interfaces. Anderson (2001) discussed the role of semiotics in user interface design and stated that semiotics is helpful for positioning the design of computer systems in a broader theoretical and philosophical context. Liu (2002) argued that as a result of the inability of users to understand the meanings of words and the inability of analysts to understand user requirements, a method with an emphasis on semantics is needed to clarify meanings to enrich communication channels. Sjostrom and Goldkuhl (2003) presented a socio-pragmatic and semiotic concept of user interfaces and argued that conceptualizing user interfaces by using the semiotic paradigm allows for understanding IS use as social action and understanding how IS artifacts can be seen as communicative instruments in such social action. And Dhillon and May (2006) used semiotics to frame an enriched understanding of information security in the context of human computer interaction (HCI).

2 SEMIOTIC FRAMEWORK FOR INFORMATION SECURITY

Semiotics is the study of signs and how they are used for information transfer between senders and receivers (Pierce, 1948; Stamper, 1973). More specifically, the field of semiotics provides a structured discipline for studying information, information flow (communication), and culture. By breaking down information flow into small units (signs), semioticians are better able to interpret the real meaning that lies beneath various forms of communication thus providing a basis for discovering the deep-rooted issues that pertain to various phenomena (Barley, 1983; Manning, 1992; Falkenberg *et al*., 1998).

Charles Morris, an American philosopher, first introduced the field of semiotics in 1901. He determined that signs can be broken down into three layers of abstraction. Morris labeled these three layers as syntactics, semantics, and pragmatics (Zemanek, 1966). In his book, *Signs, Language and Behavior,* Morris (1955) defined *syntactics* as the layer that deals with the combination of signs without regard for their specific significations or their relation to the behavior in which they occur; *semantics* as the layer that deals with the signification of signs in all modes of signifying; and *pragmatics* as the layer that deals with the origin, uses and effects of signs within the behavior in which they occur.

As the field of semiotics advanced throughout the mid to late 1900s, additional layers of abstraction were added. The semiotic ladder, an analytical tool that was first introduced in the 1970s by Ronald Stamper, represents that signs can be studied using six different layers of abstraction. These six layers can further be classified into both human and technical level issues (Stamper, 1973; Liebenau and Backhouse, 1990). The human level consists of social, pragmatic, and semantic layers, and the technical level consists of syntactic, empiric and physical layers. These layers along with their application to information security are shown in Table 1 and will be briefly discussed in the following paragraphs.[1]

[1] A more detailed discussion of semiotics is warranted but is not presented here as a result of space limitations.

Semiotic Layer	Brief Description	Information Security Issues
Human Level		
Social	System of norms, beliefs, expectations, commitments, law, contracts, values, shared models of reality, and attitudes	Alignment of mission of business, ethical environment, social implications, and security policy, with security requirements
Pragmatic	Culture, communications, intentions, and negotiations	Organizational norms and security culture; Education, training and awareness
Semantic	Meanings and consequences of human behavior	Consequences of misinterpretation of data or misapplication of rules; Responsibility and attribution of blame
Technical Level		
Syntactic	Rules, procedures, structure, and language	Software; Security reviews and audits to ensure data integrity and to handle program bugs and software piracy
Empiric	Statistical behavior, efficiency, and redundancy	Telecommunication equipment and network strategies; Virus handling and encryption
Physical	Physical domain	Hardware; Physical security

Table 1. Semiotic Framework for Analyzing Information Systems Security (Adapted from: Stamper, 1973; Liebenau and Backhouse, 1990; and Dhillon, 1997)

Physical Layer - As shown in Table 1, the physical layer lies at the bottom of the ladder. Analysis at this layer is mainly concerned with modeling the properties of information as input to and output from any physical component of an information system. Thus, hardware issues typically map to the physical layer (Falkenberg et al., 1998). At the physical layer, the term information is generally defined as a collection of tokens that have both dynamic and static properties. A dynamic token is referred to as a signal and a static token is referred to as a mark. The physical layer is thus concerned with modeling these tokens in terms of their sources, destinations, and routes over which they are transmitted. In the context of information system security, physical layer analysis requires that the appropriate hardware be determined to provide both proper information and physical security of assets.

Empiric Layer - The empiric layer views information in terms of its availability and usability. That is, the empiric layer is mainly concerned with the properties dealing with the transmission of tokens across channels of communication. Thus, telecommunication issues typically map to this layer (Falkenberg et al., 1998). Additionally, the engineering principles of noise, entropy, pattern, variety, redundancy, and efficiency would all be addressed at the empiric layer. In the context of information system security, empiric layer analysis requires that appropriate telecommunication equipment and network strategies be determined to properly handle the security needs of an organization. Additionally, virus handling and encryption strategies are determined at this layer.

Syntactic Layer - In contrast to the empiric layer, the syntactic layer is not concerned with any empirical or statistical properties of information; rather the syntactic layer is concerned with the form and shape of this information. That is, the syntactic layer is mainly concerned with the structure and form of tokens. This structure and form is expressed as syntax and requires generally agreed upon rules and formulations for consistency. Hence, software issues typically map to the syntactic layer (Falkenberg et al., 1998). In the context of information security, syntactic layer analysis requires that the appropriate software be determined that allows for proper authentication techniques, intrusion detection, vigilance, and the maintenance of consistent and available data. Additionally, proper and timely security review and audit strategies are formed to ensure data integrity and to handle program bugs and software piracy.

Semantic Layer - As shown in Table 1, the semantic layer lies at the interface of the technical and human levels of the semiotic ladder. The semantic layer is mainly concerned with meanings and is not concerned with what language is used, how the message is encoded, or by what medium any message is transmitted on. Semantic layer analysis considers various concepts such as propositions, validity, truth, signification, and denotation to uncover a rich understanding of meaning to all concerned with a particular information system. In the context of information security, semantic layer analysis requires that meanings and consequences (validation steps) of various security design issues be examined. Via this type of analysis, issues such as the consequences of misinterpreting data or misapplication of rules are determined that leads to the formation of responsibility structures.

Pragmatic Layer - In contrast to the semantic layer, the pragmatic layer is not concerned with semantic meaning; rather pragmatics is concerned with the intentions of both the sender and receiver in context. In other words, the pragmatic layer recognizes that meanings do not provide accurate or intended upon actions or reactions when taken out of context. At the pragmatic layer, communication is studied intensively and is considered to be successful when a meaningful utterance is passed by a sender with a certain intention and is interpreted by the receiver of this utterance with the same intention. As a result, pragmatic analysis tends to deal with conversations, negotiations, and intentions of the social aspect of an information system. Pragmatic analysis also helps in interpreting the patterns of behavior and obligation afforded by different stakeholders. In the context of information system security, pragmatic layer analysis reveals the need for considering the types of communications and negotiations required within the various levels of an organization (strategic, managerial, and operational) to implement various security design issues. At this layer of analysis, education, training, awareness and compliance issues are all considered.

Social Layer – As shown in Table 1, the social layer lies at the top of the ladder. Social layer analysis deals with the consequences or outcomes of pragmatic communication. That is, when a meaningful utterance has occurred, the social layer would be used to identify the social norms that would be changed, altered, or affected in some way. As shown in Table 1, some examples of these social norms might include: commitments, law, contracts, values, shared models of reality, and attitudes. In the context of information security, social layer analysis requires that the mission of the business be articulated and aligned with a viable security strategy. Via this analysis, organizational norms, ethics, and the impact of implementing various security design scenarios must be considered and used as input for developing an enriched organizational-wide security policy.

3 METHODOLOGY

The purpose of this research is to provide a holistic conception of information security via the development and validation of a conceptual framework. As previously shown, this framework (Table 1) was developed in Section 2 and was grounded by the theory of semiotics. To provide validation for this framework, a case study was then analyzed. The case study not only helped in grounding various theoretical assertions, but also in identifying information system security concerns. A discussion of such concerns helps in ensuring that all facets of information security analysis are covered. Validating the framework in this manner then allowed for the systematic uncovering of a theoretically grounded security analysis and implications for enriching security policy to emerge.

The choice of the case study was largely governed by the intent to develop a richer understanding of how various actors and technologies come into play so as to define proper information security. In this regard we proactively sought and successfully gained access to a major hotel and a casino property that had been experiencing some information system security problems. While the management was aware of the concerns and some steps had been taken to solve the security challenges, the problems persisted. We

engaged with stakeholders at different levels in the organization to better understand the root cause of the security problems. In the end, 23 interviews with various staff members were conducted. We also established a relationship with one of the key security officers who helped us in validating our findings. The study was approved by the University Internal Review Board and systematically followed Yin (2003). That is, key stakeholders were identified; interview strategies were developed prior to discussions; ethical guidelines were strictly followed; data was collected and stored in a systematic manner; and the final results were revised and verified via the solicitation of rigorous feedback procedures.[2]

3.1 Case Study Description

For purposes of anonymity, the organization in this case study will be referred to as Tower, a major hotel and casino property with six restaurants, four lounges, a pool, and a unique set of tourist attractions. Security for Tower is divided into two departments, Gaming Surveillance, and general physical Security. Gaming Surveillance is responsible for the observation of all gaming and finance operations in the casino. Security is responsible for the protection of the employees, guests, and the assets of the corporation. If Gaming Surveillance needs physical enforcement of gaming regulations, they call upon Security. Both Gaming Surveillance and Security are run by directors who report to the corporate CFO. A separate IT department with several employees and a manager is responsible for handling the technical requirements for ensuring information security.

Since the company was founded, the same management has been in place in the IT department. The management in Security has been in place since a 1995 expansion and change of ownership. Since the expansion, ego and personality clashes created a distinct animosity between the two department managers. The IT manager had on numerous occasions stated that he felt that the manager of Security was ineffective and that two different departments were not needed. In turn, the manger of Security felt that IT had interfered with the operation and confidentiality of security investigations.

These continued clashes served to interfere with the daily operations of staff. In addition to slow operations as a result of an inefficient server, in more than one instance it was alleged that information in sensitive investigations was leaked to the public or opposing lawyers. While none of these allegations could be proved, security officers often felt unnerved when, while working on a report, they would find IT personnel taking control of the "cursor on the screen." IT would explain that they were correcting someone else's problems and they needed to test the system. The Security department's answer to this was to create reports using Microsoft Word, printing them and then deleting the report from the system. While this created good-looking paper reports, they could not be corrected, added to, or utilized for analysis purposes. This solution also resulted in reports being stored in multiple filing cabinets rather than on a secure server. An unanticipated problem that occurred was that during late-night shifts the filing cabinets were not accessible to the security officers. This resulted in felons being released because officers could not show Metro Police instances of a person's prior behavior.

As a result of poor cross department relations, the conceptual model that was held by the Security Department was not the same one seen by IT. Both departments needed to interact with a system that was reliable, secure, and cost effective. Yet, the only thing that both departments could seem to agree on was that they required automation. As a result, various disjointed applications were purchased over the years to ensure security. For example, the IT manager was noted for purchasing a software package based on incomplete information. This led to data being lost as a result of the IT staff not being properly trained to

[2] Due to space limitations we are unable to discuss the nature and scope of the interviews or our philosophical stance.

enter data. Additionally, poor software selection led to unauthorized IS technicians looking at sensitive security files.

4 RESULTS

This section will describe the results obtained from analyzing the information security problems that emerged from the Tower case study. The analysis was grounded by using the semiotic framework shown in Table 1 as a theoretical basis for discovery. The presentation of these results is organized by first placing the various security problems into their corresponding semiotic layer. We then begin the presentation of our results at the social layer. As we work down the ladder, we discuss various new problems that were discovered and identify problem solving activities for each layer. Throughout this discussion, we bring attention to the need for allowing each layered analysis to inform the other layered analyses. Organizing the results in this manner allows for the systematic uncovering of a theoretically grounded and holistic analysis to emerge and provides validation to the framework presented in Table 1. Table 2 provides a synthesis of these results.

Semiotic Layer	Problems Encountered	Problem Solving Activities
Social	Ego and personality clashes affected the security operation of a major hotel casino	• Align stakeholder interest with mission of business and viable security solution
	The conceptual model for security that was held by the Security Department was not the same one seen by IT	
	Final security solution did not offer what was needed	
Pragmatic	Security solution required untrained users to be data entry specialists	• Ensure proper education, training and awareness
Semantic	Procrastination and misinterpretation of rules allowed the security implementation to fall behind and eventually fail	• Create and enforce responsibility structures - attribution of blame
	Unauthorized IS technicians accessed sensitive files	
Syntactic	IT director purchasing a software package based on incomplete information	• Enhance software analysis • Conduct timely and effective security reviews and audits
	Leaks of information to the public and opposing lawyers	
	Inadequate reports for proper security analysis	
Empiric	Slow server	• Enhance network analysis
Physical	Inadequate hardware to handle increasing data storage requirements	• Enhance hardware analysis • Create enriched data storage strategy
	Inadequate storage of reports leading to release of felons	
	Lost data	

Table 2. Semiotic Analysis of Tower Case Study (Developed Via the Theoretical Framework Shown in Table 1)

4.1 Social Layer Analysis

As shown in Table 2, three problems were encountered in the Tower case study that required an initial social layer analysis. First, ego and personality clashes between the two directors of Gaming Surveillance and Security negatively affected the security operations of this firm. Second, the conceptual model for security that was held by the Security Department was not the same one seen by IT. And third, Security was not provided a system that was truly needed; one that was reliable, secure and cost effective.

When considering these three problems in the context of the theoretical framework shown in Table 1, it was concluded that Tower should have attempted to align stakeholder interest with their mission of business and a viable security solution. That is, this organization needed to recognize when different departments have to work together to achieve the same goal, ego and personalities clashes will inevitably cause problems. Had there been a proper assessment of the cultural norms (investigating beliefs, expectations, commitments, law, values, shared models of reality, and attitudes) and political environment at Tower, proper collaboration channels (pragmatic issue) could have been established between the two departments resulting in a shared conceptual model for security. This in turn could have then provided a proper environment for properly addressing and implementing Tower's information security needs.

4.2 Pragmatic Layer Analysis

As shown in Table 2, the Tower case study provided one problem that required an initial investigation at the pragmatic layer. This problem was that the security solution that was provided required untrained users to be data entry specialists. When considering this problem it becomes clear that Tower needed to consider the technical capabilities of its existing staff and analyze techniques for correcting this issue. Via this type of analysis, a proper plan that aligned the current capabilities of existing employees with their current security needs could have then been developed.

When considering this problem in the context of the theoretical framework shown in Table 1, it was concluded that Tower should have created a strategy for providing proper education, training and awareness of all users. This strategy would then be aligned with and improved upon in an iterative manner by considering the results obtained in the various other layered analyses. For example, results from the social layer analysis enhanced the comprehension of how to align the security needs of the organization with various stakeholder interests. This type of analysis would then allow for a better understanding of the social environment at Tower and would lead to an enriched training and awareness strategy.

4.3 Semantic Layer Analysis

As shown in Table 2, the Tower case study provided two major problems that required an initial investigation at the semantic layer. First, procrastination and lack of follow-up allowed for the security implementation to fail. Second, unauthorized IS technicians were capable of accessing sensitive files. When considering these two problems in the context of the theoretical framework shown in Table 1, it was concluded that Tower could have overcome these issues by creating a meaningful system of responsibility structures so that individuals in the organization could be held accountable for various issues. A clear designation of who is responsible for what would have then led Tower management to the creation of a system for attributing blame thus keeping motivation alive to get the job done right, on time, and in an ethical and lawful manner.

4.4 Syntactic Layer Analysis

As shown in Table 2, the Tower case study provided three problems that required an initial investigation at the syntactic layer. First, the IT director purchased software based on incomplete information. Second, sensitive information was leaked to the public and opposing lawyers. And third, reports were inadequate for the purposes of proper security analysis. When considering these three problems it becomes clear that the problem of the IT director purchasing software based on incomplete information resulted from earlier problems such as ego and personality clashes and a disjointed conceptual model for security. No doubt, the IT director should not be independently choosing software without a full analysis of what is required.

And as has been shown, this analysis transcends a techno-centric perspective. Had a proper software analysis been performed, the purchase of software would have resulted from an organizational perspective and might have prevented sensitive information from being leaked and for proper reports to have been created.

Thus, when considering these three problems in the context of the theoretical framework shown in Table 1, it was concluded that Tower should have considered two problem solving activities. First, an adequate software analysis should have been performed. And second, Tower needed to create a system that ensured timely and effective security reviews and audits. An adequate software analysis should have been grounded by the human level issues that emerged at the social, pragmatic and syntactic layers and combined with a proper technical analysis. To ensure that the issues of information leaks and poor reports did not occur in the future, a timely and effective auditing strategy for reviewing current states of security should have then been created.

4.5 Empiric Layer Analysis

As shown in Table 2, the Tower case study provided one major problem that required an initial investigation at the empiric layer. This problem was that proper security could not be maintained as a result of a slow server. When considering this problem in the context of the theoretical framework shown in Table 1, it was concluded that Tower should have performed an adequate network analysis where the efficiency of the overall system was considered. And again, an adequate analysis at this level required considering all of the lessons learned from previous layered analyses and allowing the output from this layer to improve upon earlier progress.

4.6 Physical Layer Analysis

As shown in Table 2, the Tower case study provided three problems that required an initial investigation at the physical layer. First, a lack of adequate hardware to handle increasing data storage requirements was noted. Second, inadequate electronic storage capability of reports led to felons being released. Third, important data was lost. When considering these three problems in the context of the theoretical framework shown in Table 1, it was concluded that Tower should have considered two problem solving activities. First, an adequate hardware analysis should have been performed. Second, Tower needed to create an adequate data storage strategy.

5 DISCUSSION

Several researchers have called for developing holistic models for conceptualizing information security where both social and technical perspectives are considered (Eloff and Eloff, 2003; Anderson, 2007; Zucatto, 2007; Kritzinger and Smith, 2008). However there have been problems in the past with defining such models. This was largely because information security is multidisciplinary and any model at best helps in addressing issues in part or from a single dimension. As contended earlier, semiotics offers a meta-theoretical basis for defining a holistic understanding of information security. In this light, we defined such a basis and presented it in Table 1. We then used the concepts therein to undertake a case study. The case analysis not only helped in validating and further refining the framework, but in identifying pertinent issues that need to be considered in information security management.

Interestingly enough, the security problems identified in the Tower case study could be described and analyzed through the semiotics based framework. And for each problem that was analyzed, a problem solving activity emerged. For example, social layer analysis indicated that had Tower adequately aligned stakeholder interest with their business mission and a viable security solution, then the three problems

that included ego and personality clashes, a disjointed conceptual model for security across departments, and the lack of a system that met Tower's information security needs, could have all been remedied. In the literature, ego gratification has been positively linked with information security breaches (see Shaw et al 1998) as has been a lack of structure across organizational units (Baskerville and Dhillon, 2008).

As the investigation in Section 4 worked its way down the ladder, the individual layered analyses not only served to solve the individual problems at each layer, but were further used to enrich earlier solutions via an iterative approach. For example, it was found that an adequate software analysis should have been grounded by the human level issues that emerged at the social, pragmatic and syntactic layers and combined with a proper technical analysis. This result is in-line with Dhillon (1997, pg.37) where he contends that human level analysis serves to enrich the picture of the problem domain, and after a human level analysis has been conducted, the technical level issues can then be examined to a deeper extent.

5.1 Enriching Security Analysis and Policy Formation

The results in Section 4 alluded to an iterative approach for enriching information security analysis. However, with so many issues to consider, no single security problem was given a complete ladder analysis at all six layers. Additionally, policy formation has yet to be discussed. Thus to provide a clear picture of how the conceptual framework shown in Table 1 can be used to enrich security analysis and security policy formation, an illustrative example (Figure 1) will briefly be discussed.

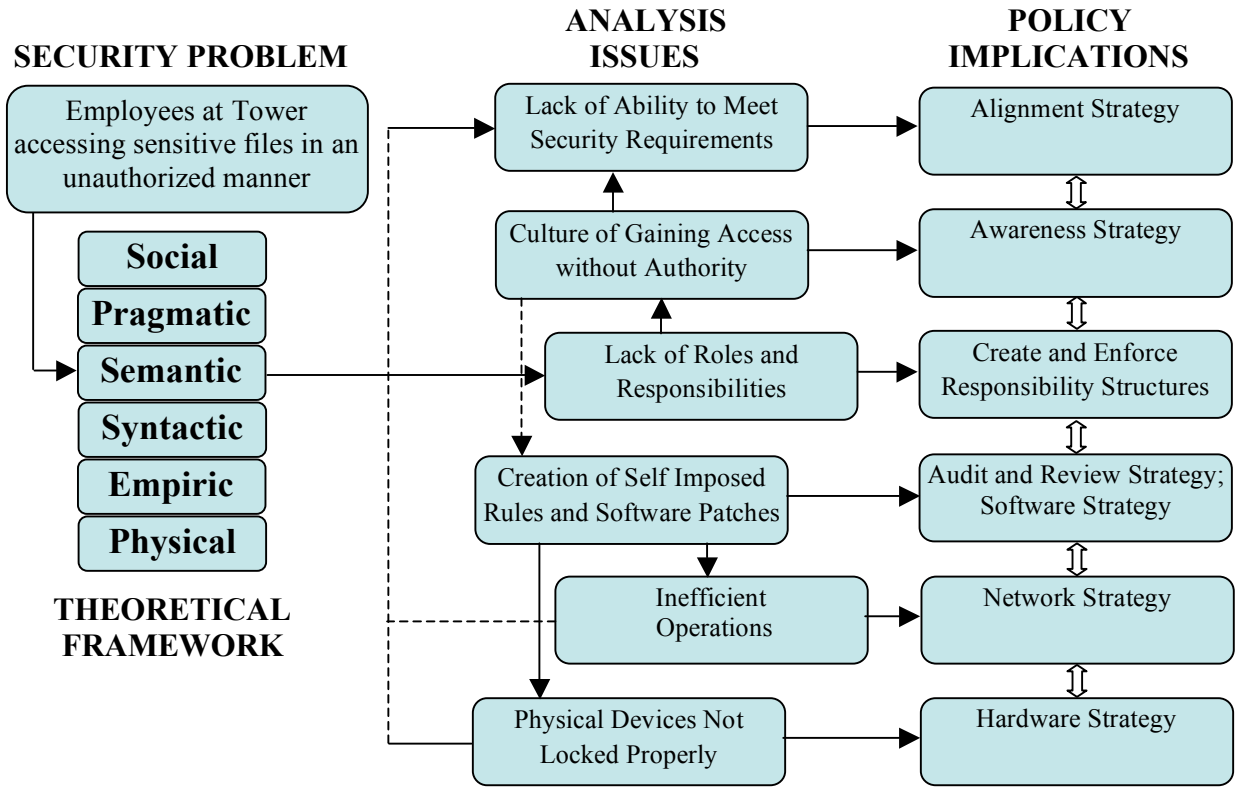

Figure 1. Detailed Analysis of One Tower Security Problem

As shown in Figure 1, the starting point for any analysis could be the theoretical framework. Considering the issue of employees accessing sensitive files in an unauthorized manner, one can argue that this clearly results from a lack of a clear definition of roles and responsibilities. And as Backhouse and Dhillon (1996) have argued, this is a semantic issue. Perhaps the stakeholders are not recognizing the intricacies involved in a clear definition of responsibility structures and are thus more inclined to misinterpret them. Past research has shown (see Stein, 2000) that when organizational structures are weak or when the roles have not been properly delineated, a culture of lax security emerges (e.g. see Schlienger and Teufel, 2003). A weak information security culture essentially means that the business environment is not conducive to sustained productivity. In arguing about the importance of information security as a key enabler of business, Dhillon (1997, pg. 137) states:

> If we accept that secure information systems enable the smooth running of an enterprise, then what determines the ability of a firm to protect its resources? There are two routes. Either, a firm considers security as a strategic issue and hence operates in an environment designed to maintain consistency and coherence in its business objectives, or, a firm may position itself such that it gains advantage in terms of the risks afforded by the environment.

Thus, our analysis of information security issues using the semiotics-based framework shown in Table 1 helps in spotting "hot spots". These “hot spots” can then be used as a basis to, as Liebenau and Backhouse (1990) puts it, "move up and down the ladder" to conduct a deeper and more enriched analysis. For example, Figure 1 indicates that a lack of roles and responsibilities leads to a culture of gaining access without authority at Tower which then affords an environment where self imposed rules for software patches and upgrades become prevalent. This in turn results in an environment of inefficient operations and one where physical devices are not properly secured.

Figure 1 also illustrates how all of these issues generated via one Tower security problem then led to substantial implications for an enriched security policy. Tower’s lack of ability to meet security requirements provides insight for an alignment strategy. Their cultural problems provide insight for developing an awareness strategy. A lack of roles and responsibilities produces the need for developing a system for creating and enforcing responsibility structures. Self imposed rules provide insight for properly creating audit review and software strategies. The inefficient operation of Tower’s server provides insight for an enriched network strategy. And the lack of proper locking techniques for physical devices provides insight for an enriched hardware strategy.

6 CONCLUSIONS

Information security is becoming a multidimensional discipline where both social and technical considerations must be considered in a coherent manner. Thus, the need for creating holistic models for conceptualizing information security in this light has been established in the literature. As a result, this research presented and discussed such a conceptual model that was grounded by the theory of semiotics. We then validated our model through the use of a case study. In addition to validating our framework, the problems discovered in the case analysis served to identify a number of problem solving activities that need to be considered in information security management. Additionally, this research indicated that when security problems are forced through a systematic investigation up and down the layers of our conceptual framework, an enriched security analysis and implications for an enhanced security policy emerge.

References

Andersen, P. B. (1992). Computer semiotics. Scandinavian Journal of Information Systems, 4, 3-30.

Anderson K. (2007). Convergence: a holistic approach to risk management. Network Security, 5, 4–7.

Backhouse, J. and Dhillon, G. (1996). Structures of responsibility and security of information systems. European Journal of Information Systems, 5(1), 2-9.

Barley, S.R. (1983). Semiotics and the study of occupational and organizational cultures. Administrative Science Quarterly, 28(3), 393-413.

Baskerville, R. and Dhillon, G. (2008). Information Systems Security Strategy: A Process View. Information Security: Policy, Processes, and Practices. D. W. Straub, S. Goodman and R. Baskerville. Armonk, NY: M E Sharpe.

Braf, E. (2001). Knowledge or information – What makes the difference? In Liu, K., Clarke, R. J., Andersen, P. B., Stamper, R. K. (eds.), Organizational Semiotics – Evolving a Science of Information Systems, Deventer, The Netherlands: Kluwer Academic Publishers, 119-1321.

Dhillon, G. (1997). Managing Information System Security. London: Macmillan.

Dhillon, G. and May, J. (2006). Interpreting security in human computer interactions: A semiotic analysis. In Human-Computer Interaction and Management Information Systems – Foundations. Eds Zhang, P. and Galletta, D, M. E. Sharpe, Inc.

Dhillon, G. and Torkzadeh, G. (2006). Value focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Dlamini, M.T., Eloff, J.H.P. and Eloff, M.M. (2009). Information security: The moving target. Computers & Security, 28(3-4), 189-198.

Eloff J.H.P. and Eloff, M.M. (2003). Information security management – A new paradigm. Proceedings of SAICSIT, 130 –136.

Falkenberg, E., Hesse, W., Lindgreen, P., Nilsson, B., Oei, H., Rolland, C., Stamper, R., Van Assche, F., Verrijn-Stuart, A., and Voss, K. (1998), A framework of information system concepts. International Federation for Information Processing (IFIP), Laxenburg, Austria.

Herath,T. and Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47, 154–165.

Kritzinger, E. and Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers & Security 27(5-6), 224-231.

Liebenau, J. and Backhouse, J. (1990). Understanding information. Basingstoke: Macmillan.

Liu, K. (2002). Semiotics for information systems engineering – Reduce the gap between specification, design, and implementation. 1st Int. Workshop on Interpretative Approaches to Information Systems & Computing Research, 62-65. Brunel University.

Manning, P. (1992). Organizational Communication. New York: Aldine de Gruyter.

Morris, C. (1955). Signs, Language, and Behavior. New York: G. Braziller.

Nadin, M. (1997). A Semiotic Introduction to Systems Design, Cambridge University Press.

Peirce, C. S. (1948). Collected Papers. Four Volumes. Harvard University Press.

Rainer, R. K., Marshall, T. E., Knapp, K. J., and Mongomery, G. H. (2007). Do information security professionals and business managers view information security issues differently? Information Systems Security, 16(2), 100-108.

Schlienger, T. and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. In Proceedings of 14th International workshop on Database and Expert Systems Applications, September 1-5.

Shaw, E. Ruby, K. G. and Post, J.M. (1998). Insider Threats to Critical Information Systems, Technical Report #2; Characteristics of the Vulnerable Critical Information Technology Insider (CITI). Political Psychology Associates, Ltd., June.

Sjostrom, J., and Goldkuhl, G. (2003). The semiotics of user interfaces–a socio-pragmatic perspective. 6th International Workshop on Organizational Semiotics, Reading, UK.

Stamper, R. (1973), Information in Business and Administrative Systems. London: Batsford.
Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005). Analysis of end user security behaviors, Computers & Security, **24** (2), 124-133.
Stein, M. (2000). The risk-taker as shadow: a psychoanalytic view of the collapse of Barings Bank. Journal of Management Studies, 37(8), 1215-1228.
Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO 17799. Computers and Security 24(6), 472–484.
Yin, Robert K. (2003). Case Study Research: Design and Methods. London: Sage Publications.
Zemanek, H. (1966). Semiotics and programming languages. Communications of the ACM, 9(3), 139-143.
Zuccato A. (2007). Holistic security management framework applied in electronic commerce. Computers and Security, 26 (3), 256-265.