Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

A Semantic Analysis of Security Policy Formulation and Implementation: A Case Study

Michael Lapke
Virginia Commonwealth University

Gurpreet Dhillon
Virginia Commonwealth University

Recommended Citation

Lapke, Michael and Dhillon, Gurpreet, "A Semantic Analysis of Security Policy Formulation and Implementation: A Case Study" (2006). *AMCIS 2006 Proceedings*. 166.
http://aisel.aisnet.org/amcis2006/166

A Semantic Analysis of Security Policy Formulation and Implementation: A Case Study

Michael Lapke
Virginia Commonwealth University
lapkems@vcu.edu

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

ABSTRACT

This study is aimed at understanding how multiple perspectives of stakeholders are incorporated in the formulation of security policy. The research was guided by the Theory of Semantics. A framework was created from established semantic theory. Guided by the framework, a case study was carried out at a large state University. The point of the case study was to provide insight into security policy formulation. This insight may guide researchers in developing principles for effective security policy design. The development and implementation of this framework of semantic analysis is the major contribution of this paper. This framework could also help future researchers pursue semantic research.

Keywords

Security, policy, semantic analysis, policy formulation, policy implementation

INTRODUCTION

The way in which security policy is created and implemented is fraught with potential problems that are difficult to measure. What a security officer may have intended could be worded to imply a completely different intent. On the other end of the spectrum, a policy may be interpreted by a system user in an unexpected manner. Either or both of these potential scenarios can lead to a disconnect between security policy formulation and security policy implementation. In practical terms, this disconnect defeats the very purpose of the security policy.

According to a 2004 study, only 37 percent of executives surveyed said that their organization had both measured and reviewed the effectiveness of its security policy and procedures while 31 percent said they reviewed only (Cosgrove, 2004). Furthermore, One-quarter (24%) of companies surveyed had neither measured nor reviewed the effectiveness of their security policies and procedures (Cosgrove, 2004). This lends credence to the point that many of the decision makers within an organization would not be aware of a disconnect. The same study reported that only 50 percent of users are in compliance with their company's security policy.

The question may be asked as to why all of this is a problem. Some might argue that if an employee just uses common sense, most security issues will not come about in the first place. Given the complexity of organizations, at a technological and social level, this is not a reasonable perspective. Organizations have attempted to deal with this in a continuously evolving manner. If one examines the first of the three generations of security development described by Baskerville (1993), it is apparent that securing an organization's information system is an extremely complex venture. The first generation, while the simplest of the three, was still a multifarious venture including unwieldy specifications that were hard to read, understand, and maintain" (Baskerville, 1993). There were a variety of lists, some approaching 1,000 potentially subjective and vague items. Despite their seemingly thorough nature, Baskerville (1993) describes a major weakness of checklists in that they oversimplify the security considerations that arise in more complex information systems.

More critical to the policy issue is the fourth generation of security development described by Siponen (2001); behavior and responsibility. Responsibility, defined as the "relationship between two agents regarding a specific state of affairs, such that the holder of the responsibility is responsible to the giver of the responsibility, the responsibility principal" (Siponen, 2001, page 129) is implied in the very existence of a security policy. A policy informs a user of their responsibilities regarding an Information System's use. Assuring a proper line of communication between the makers of the policy and the users of the policy is essential or said responsibility may never be properly understood or properly articulated.

BACKGROUND

The issue of security policy has been examined from several different perspectives in IS literature. Willison (2002) examined security policy through the lens of criminal opportunity. With the premise that 52% of all logistical and physical security breaches arose from the activities of personnel within the organization, effective controls are essential (Willison, 2002). These controls, in the form of security policy, formally define security requirements, outline the main security objectives, and allocate responsibilities (Willison, 2002). Willison (2002) calls for the enlightenment of staff to their responsibilities as outlined in the security policy to maximize the probability of compliance.

There has also been research which looks into specific areas within the realm of security policy. Ahmad and Ruighavar (2003) called for the improvement of audit management technology to allow administrators to configure the software to reflect the security needs of an organization as defined in the security policy. Changing the configuration from the status quo bottom-up approach to a policy-centric top-down approach would help the configuration more closely match an organization’s security goals (Ahmad and Ruighavar, 2003). Schneider (2000) addressed the issue of enforcement mechanisms for application-dependent and special-purpose security policies. Application-dependent scenarios might include information leakage via mobile code, fraud via electronic commerce, or intellectual theft via electronic storage and retrieval of intellectual property.

On the other end of the security policy spectrum are multi-policy systems. These are defined by Kühnhauser (1999) as systems that support a multitude of independent security domains in which an individual security policy is enforced on the applications. Kühnhauser performed a logical analysis to introduce a formal model of policy groups. Joshi, Ghafoor, and Spafford (2001) also discuss the issue of multi-policy systems by examining the emerging “digital government.” A sequence of solutions to the issues of multi-domain environments are presented including ad hoc approaches, formal approaches (with reference to Kühnhauser), model-based methods, agent-based methods, architectural methods, and the database federation approach (Joshi, *et al*., 2001).

Regarding policy formulation, the variety of approaches in the research literature demonstrates the multifaceted nature of the phenomenon. At the practitioner level, Rees, Subhajyoti, and Spafford (2003), aimed to provide information security professionals and top management a framework through which useable security strategy and policy for applications can be created and maintained in line with the standard information technology life cycle. This framework was cyclical in nature and consisted of four stages, plan, access, operate, and deliver. At the theoretical level, Glasgow and Macewen (1992) created a formal framework for specifying security policies. This framework, called Security Logic, defines what a subject knows, what information a subject has permission to know, and what information a subject is obligated to know. The paper presented this via a logical approach based on modal logic formalism (Glasgow, *et al*., 1992). Baskerville and Siponen (2002) specifically tackle the issue of policy formulation by way of calling for a security meta-policy. They note the fact that existing security policy approaches do not pay much attention to policy formulation itself. In other words, the actual creation of the policy is done in an ad hoc manner.

Security policy implementation studies tend to be disaster focused. Coyne and Kluksdahl (1994) examined a failed security policy implementation and found that compliance-based approaches are more prone to failure than risk-based approaches. This study detailed the scenario at the National Aeronautics and Space Administration (NASA) when the Department of Defense (DOD) terminated its involvement with the agency. With the Mission Control Center (MCC) no longer bound to comply with DOD’s mostly unrelated regulations, a new organization was established to develop the new security policy. The new organization was external to normal operations and did not deal with requirements relating to budget and operational issues. This resulted in a de-facto compliance-based policy which led to the reaction of all security related matters being adversarial in nature (Coyne, *et al*., 1994). To combat this issue, Coyne, *et al*., (1994) call for a risk-based approach, centered in the development organization but with close ties to the operational organization, budget factors, scheduling, and operational factors. This new perspective would allow for a better evaluation of system security requirements and implementations. This work contrasts the underlying assumption in Willison’s (2002) previously cited work that compliance is the ultimate goal of a security policy.

While all of this research provides for insight into the issue of security policy, it does not explore how to analyze stakeholder interpretations of such policy. It is hoped that the analysis provided in this paper will give an opportunity for researchers to shed light into this phenomenon. A method for such an analysis is presented in the following section.

A THEORETICAL FOUNDATION FOR A CONCEPTUAL FRAMEWORK OF SEMANTIC ANALYSIS

The primary source of information for Semantic Theory will come from a semiotic perspective. According to Anderson (1990), semiotics is the science of sign systems including linguistics, as well as the study of all other sign systems. Semiotics also includes the general principles that underlie all sign systems. It is thus more comprehensive than linguistics; much more, because there is a semiotic dimension to practically every human artifact (Anderson, 1990). This makes the semiotic approach quite appropriate to investigating Information Systems. Several IS researchers have made use of the semiotic approach including Anderson (1990), Ulrich (2001), and Stamper (1973).

Stamper (1973) presents a framework for semiotics that breaks down information into four different "levels." These are empirics, syntactics, semantics and pragmatics. They represent a spectrum of information that moves from the natural world to the social. Semantics resides between the rules of syntactics but below the affected behaviors of pragmatics. It is representative of the *meanings* of signs. Hence, semantic theory must provide a representative scheme for what constitutes meanings (Katz, 1970). Stamper (1973) provides a concise and elegantly simple semantic model, as part of his overall semiotic model, that one can use to build a framework in which all dimensions of meaning can be explained.

Stamper (1973) describes four approaches to meaning in the semantic sense: denotative descriptions, affective descriptions, denotative prescriptions, and affective prescriptions. Denotative descriptions are simply a statement of something that exists. Stamper (1973) states that "designative signs must be justified by showing their relationships with things which can be observed by anyone." This indicates a low level of subjectivity. Morris (1970) also describes this by stating that designative signs help gather relevant information regarding the nature of the environment in which the organism operates. Further demonstrating the high objectivity of it, Stamper (1973, page 75) describes denotative descriptions as being "easy with a physical object, difficult with a statement about a past event."

The second semantic element, affective descriptions are those that are more based on subjective feelings and human values. Stamper (1973, page 75) describes them as "value judgments: reports on staff, estimates of the relative difficulties of jobs." Stamper (1973) describes a key, distinguishing, characteristic of affective information, as referring to individual human feelings. Stamper (1973, page 75) does give credence to this subset of semantics by stating that "only by reference to the human organism and its power of appraisal can we justify designating a supposed pattern of data as a thing." Morris (1970) describes affective descriptions as how the actor can transfer his choice of an impulse-satisfying object from the consummation phase to the orientation phase.

A new area is uncovered in the next semantic element, denotative prescriptions. The first two dealt with how a sign is described. This element and the next one differ from descriptions in that they are directive. Stamper (1973, page 77) describes them as "an order, a rule or a recommendation that will denote the objects to which the prescribed action must be related." Morris (1970) states that prescriptive signs guide the actor's behavior according to the ways in which the organism must act upon the environment in order to satisfy its need. Going beyond directives, Stamper also addresses consequences as critical: "they depend heavily on sanctions that can be imposed or rewards that can be granted" (Stamper, 1973, page 77).

The final semantic element, affective prescriptions, takes the directive approach and mixes the human element. According to Stamper (1973), words may have the superficial appearance of a command or law. The key is that their prescriptive standing is only justifiable in so far as they arouse expectations about the consequences of obeying or disobeying them. The human element however is not only indicative of those that prescribe but also those who are prescribed upon. Stamper (1973, page 78) demonstrates this by stating "what sanctions can be applied very largely depends upon the consent of those to whom they are supposed to apply."

Stamper (1973), Morris (1970), and Katz (1970) have clearly delineated the meaning of semantics, which itself is the study of meaning. By looking at the concrete ways in which an object or artifact is described, the subjective way an object or artifact is described, the concrete way rules about that object or artifact exist, and the subjective interpretation of those rules, one can get a clear semantic understanding of that given object or artifact. The dimensions of semantics outlined in this section are condensed into a framework that can be used for future research on ISSP formulation. This semantic framework is presented in Table 1.

Semantic Element	**Description and seminal works**	**Semantic Issues in Security Policy Formulation**	**Semantic Issues in Security Policy Implementation**
Denotative Descriptions • Designation • Facts • Evidence • Forecasts	This semantic element is simply a statement of something that exists. (Stamper, 1973) The nature of the environment in which the organism operates."" (Morris, 1970).	What are the known current vulnerabilities of the system in question? How technically secure is the IS in its current state? How physically (and socially) secure is the IS in its current state? How many and what kind of security incidents have occurred with the current system?	Is the security policy in place easily accessible by the users and IS staff? Is the security policy required reading for all the users of the system? Are the security policy procedures actually followed by the IS users?
Affective Descriptions • Appraisals • Value • judgments	Value judgments: reports on staff, estimates of the relative difficulties of jobs. (Stamper, 1973) How the actor can transfer his choice of an impulse-satisfying object from the consummation phase to the orientation phase. (Morris’ 1970)	What is the current sentiment among the IS staff about the level of security with the IS? Do the IS users feel that the current level of security is acceptable? How much of a burden do the IS users feel the current security measures cause?	Is the security policy written in simple language that most (non-technical) users could easily understand? Are the procedures detailed in the security policy ridiculed or readily accepted by the IS users (i.e. regular password changing is rarely followed)?
Denotative Prescriptives • Instructions • Plans • Policies • orders	An order, a rule or a recommendation that will denote the objects to which the prescribed action must be related. (Stamper, 1973) Guide the actor's behavior according to the ways in which the organism must act upon the environment in order to satisfy its need. (Morris, 1970).	How does the current security policy handle non-compliance? Are the consequences for non-conformation to the security policy included in said policy?	Are IS users aware of the specific security policies in terms technical security? Are IS users aware of the specific security policies in terms of social security?
Affective Prescriptives • Inducements • Coercion • Threats • rewards	“Words may have the superficial appearance of a command or law but their prescriptive standing is only justifiable in so far as they arouse expectations about the consequences of obeying or disobeying them.” (Stamper, 1973)	If the consequences are included, are they judged to be a sufficient deterrent? How much of a burden is security policy enforcement?	Have any personnel that have broken security policy actually been punished? If they have been punished, are any of them repeat-offenders?

Table 1, Conceptual Framework for Semantic Analysis

METHODOLOGY

This research was conducted via an interpretive case study in the Information Technology Department of a large state University in the southeastern portion of the United States. Approximately two dozen employees work for this department. The research is “aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context” (Walsham, 1993). The aim of this type of research is to build a theoretical foundation and identify elements that affect the phenomena under study.

Data was gathered by way of interview. The subjects were the stakeholders involved in the formulation of the ISSP. The interviews were grounded by the previously discussed framework. The framework provided a structured foundation to the interviews but there was an open end to the interviews as well. The term structured here refers to the interviews being guided by a set of framework-prepared questions. The open-ended aspect occurred by way of the interviewer allowing the interviewees to veer their answers to any tangents they feel are important. This open ended nature helped facilitate affective aspects. As discussed in the framework, affective aspects refer to subjective value judgments. Immediately after each of the interviews, the investigator debriefed. This process of immediate “debriefing” helped clarify the researcher’s interpretations and deepen his level of understanding (Walsham, 1993).

Besides gathering data, the interviews served as subject recruitment opportunities. The process of building the network of interviewees was done in a “referral” manner. This means that the interviewees themselves will point the researcher to the next best contacts in which to continue the interview process. The point of saturation became apparent when the same names began to appear. This concept of saturation is discussed by Walsham (1993).

Once the interview process was complete, the data was interpreted by the researcher (Walsham, 1993). This process involved a systematic analysis and categorization of the data by emergent themes that the researcher identified. These themes were not known *a priori* but emerged as the data was categorized by thematic principles. The result of this process is explored in the Discussion section.

CASE STUDY

The case study took place at the previously described University in the summer of 2005. The recruitment strategy involved fostering a growing communicative network starting with a single participant. This participant is a known associate or “insider” (Walsham, 1993). With her technical position in the University, she is in a situation where she knows individuals who are most directly tied to the process of security policy formulation. This network of participants became saturated towards the end of the study, giving complete coverage of the process. By the end of the study, the total number of participants totaled 11 subjects. These were all of the people involved in the formulation of the IS Security Policy at the University under study. The discussion of the Case Study section is divided into four subsections which are guided by the semantic framework.

Denotative Descriptions

The first semantic element, as discussed in the semantic theory section, is denotative descriptions. Given the concrete nature of this element, in that it is simply a statement of something that exists, it was relatively straightforward to devise areas of exploration concerning policy. Regarding policy formulation, questions included the following: How secure is the system in question? What are the current known vulnerabilities of the system? How many and what kinds of security incidents have occurred with the current system? On the policy implementation side, the questions were as straightforward in content but actually more difficult to answer. These included the following: Is the security policy in place easily accessible by the users and IS staff? Is the security policy required reading for all the users of the system? Are the security policy procedures actually followed by the IS users?

The Information Security Officer interviewed at the organization was relatively vague in his answer regarding the level of security of the system. Specifically, he stated that “It’s as secure as it can be in our University environment. We don’t want to lock everything down but we don’t want to be attacked either.” This strongly speaks towards a lack of control over the control itself as described by Baskerville, *et al.* (2002). The response would also seem to imply that it is not secure due to restrictions imposed in what is designed to be an open environment. This interpretation was reinforced by a number of relatively serious incidents described by the interviewee. Users of the system continuously violate policy by downloading copyrighted material (particularly music) through the University network. University servers are routinely hacked by outside entities. In another example, users disregard policy by opening executable attachments to email. The consequences to the University network are catastrophic at times due to the inevitable viruses and worms that are ahead of the virus definitions of the virus scanners. On the implementation side, some of the lower level network administrators were interviewed. It was quite surprising that none of them were even aware that a specific security policy even existed. One of the administrators stated that "we could probably make [the policy] more visible. If an IT administrator wanted to find, they wouldn't have much of a problem." What further intensifies the issue is that the policy is in fact required reading by all users of the system. When an account is created, a user has to certify (by placing an 'x' in a box next to a statement saying they read the policy) that they have read the security policy. If the relatively savvy and experienced network administrators ignored this, it is pretty clear that the average user would as well.

Affective Descriptions

Affective descriptions make up the second semantic element. This deals with issues that are more based on subjective feelings and human values. Regarding policy formulation, the following types of questions would need to be addressed: What is the current sentiment among the IS staff about the level of security with the IS? Do the IS users feel that the current level of security is acceptable? How much of a burden do the IS users feel the current security measures cause? Because policy tends to be a behind-the-scenes issue with many users, gauging emotional reactions is slightly more difficult. None-the-less, the areas identified included determining whether the security policy was written in simple language that most (non-technical) users could easily understand and whether the procedures detailed in the security policy are ridiculed or readily accepted by the IS users.

The unique environment of the organization, in that it is a state University, affected this area of the semantic analysis. According to the Chief Information Officer (CIO), "most of the staff is unaware of most security related things that go on." This lack of awareness (Trompeter and Eloff, 2001; Willison, 2002; Schultz, 2004) can lead to significantly negative consequences. The CIO went on to say that "there's a pretty laid back attitude here." It seems though that this attitude reverses quite quickly when additional security measures are suggested. Prior in the paper, an example of poor security was presented via users opening and distributing executable email attachments. Given the lag of virus definitions to keep up with the incredibly fast distribution of new viruses, this practice often caused disastrous results. The security officer (with the consent of the policy committee) decided to formulate a policy which would ban all zipped and executable attachments. According to him, "this was met with tons of negative feedback and endless arguing [by the general user population]." It wasn't until a particularly powerful worm wreaked havoc to the University system that everyone began to agree this would be a good idea. The security officer summed up the feelings of users towards security measures by explaining that "there is a universal response to security measures: You're making my job harder." This phenomenon of resistance to security measures has not been thoroughly hashed in security literature. Furnell, Dowland, Illingworth, and Reynolds (2000) looked into user acceptance towards authentication. Huston (2001) analyzed the security issues with the implementation of E-Medical records and how they may be resisted by the user base.

Denotative Prescriptions

The next major area of semantic analysis takes a step away from descriptions and moves towards prescriptions. The first kind of prescriptions, denotative, is an order, a rule or a recommendation that will denote the objects to which the prescribed action must be related. This is addressed in policy formulation by determining how the current security policy handles data security issues (confidentiality, data integrity, and availability) and how it handles social security issues (responsibility, integrity, trust, and ethicality). For policy implementation, it should be determined if IS users are aware of the specific security policies in terms social and technical security.

Examination of the security policy artifact reveals that it does have extensive guidelines regarding technical security. For example, it is quite detailed describing which ports should be shut and which ones should be open on servers, which applications should be restricted, and blocking executable attachments in emails to name a few. It also discusses many socially related security issues. For example, it states "Accounts and passwords may not be shared with, or used by, other persons within or outside the University." Most of the language is vague though regarding social issues. Examples of this vague language include "Respect for the rights of others is fundamental to ethical behavior," "Actions that impede, impair or otherwise interfere with the activities of others are prohibited," and "the University may require users to limit or refrain from specific uses." This vagueness is damaging because it fails to account for the fourth generation of security development specified by Siponen (2001). On the implementation side, the CIO stated that users are "probably not consciously aware of most of the specific issues." This is reinforced by interviews with network administrators and users of the system. None of them were actively aware of a security policy, much less of the details of such a policy.

Affective Prescriptions

The final part of the semantic analysis, affective prescriptions, deals with the consequences of obeying or disobeying the prescriptions discovered in the previous portion. On the policy formulation side, this can be answered by determining if the consequences for non-conformation to the security policy included in said policy and if the consequences are included, are they judged to be a sufficient deterrent? Regarding policy implementation, it should be established if any personnel that have broken security policy actually were punished. Also, if they have been punished, are any of them repeat-offenders?

The policy artifact does include references to consequences but only regarding severe digressions. For example, the policy states that "actions that threaten or cause harm to other individuals are violations of both [University] policies and of [state] and federal law. Such actions may be prosecuted through both the University judicial process and, independently, in state or federal court." This is a scenario that is probably outside of the realm of typical IS security concerns but needs to be addressed, none-the-less. It also states that "violations of copyright, licenses, personal privacy, or publishing obscene materials or child pornography may result in civil or criminal legal actions as well as University disciplinary actions." Again, the consequences are either vague or outsourced to an agency that has clearly defined methods for consequences (i.e. the legal system). Going back to the copyright infringement issue, the way the University deals with this is by first shutting down the network connection and then counseling the student. Once the counseling is complete, the network connection is reestablished. A student can commit this digression over and over and receive the same minimal consequence every time. The security officer stated "What can we do? We're really at a loss with how to deal with problems. It's not like the bulk of the users work for the organization. Anyway, they are the ones who will be sued by the copyright owner so that should be deterrent enough." This blasé attitude is dangerous in that it completely misses the point in providing disincentives against non-compliance and the compound effect of these sanctions on others from a lack of compliance (Straub, 1990).

Wrapping up the Case Study

The interviews and document reviews conducted over the course of this case study shed considerable light on the policy formulation and implementation at this particular organization. Granted, it is a unique scenario, but it is indicative of the problems faced by organizations formulating and implementing policy. Ensuring users are aware of, read, and actually follow security policy is a challenging task. Coming up with good and effective policy is critical though. This is discussed in the following section.

DISCUSSION

In the analysis of the case study data, five emergent themes were identified. These themes clearly had a significant impact the hypothesized disconnect between security policy formulation and security policy implementation. The denotative descriptions phase of semantic analysis revealed the organization had a lack of control over the control itself. The term control is being used interchangeably with policy and the lack of control demonstrated that a deliberate and concise control mechanism is necessary. Baskerville, *et al.* (2002) describe this deliberate control mechanism as a meta-policy, or that which defines who is responsible for making policies, and when such policymaking should take place. Three imperatives are defined that a meta-policy needs in order to be effective. These include suppleness, political simplicity, and being criterion-oriented (Baskerville *et al.*, 2002). The suppleness describes the ability for a quick reaction to changing environments or organizational realities. Political simplicity can aid suppleness. This is described by defining the political goal of organizational meta-policy as maximizing "policy compliance without totally outlawing non-compliance where situations warrant" (Baskerville *et al.*, 2002, page 8). The final imperative, criterion-oriented, is described as having the policy makers have an explicit focus on the priorities of the organization. Enacting a meta-policy as described by Baskerville *et al.* (2002) could alleviate the ambiguity demonstrated by the makers of the security policy at this particular organization.

The most frequently occurring theme appeared during the investigation of the denotative description, affective description, and denotative prescription areas of semantic analysis. This was the issue of lack of awareness of the security policy. This is not a problem unique to this organization as Willison (2002) points out that in a 2001 survey, only one third of organizations provided any form of security awareness training. He goes on to state that "unless the policy is brought to life through education and awareness programs, then all the work undertaken to create a policy will ultimately have been a waste of time" (Willison, 2002). Trompeter and Eloff (2001) describe the acute need for creating and heightening socio-ethical information security awareness. Trompeter and Eloff (2001, page 386) state that "the onus, therefore, solely rests with an organization to create this socio-ethical awareness in every one of its members and among all its clients and affiliates." This can be best done through the education and awareness programs described by Willison (2002). Of course, if such a program is not already in place, it is not likely an organization will immediately be willing to spend the resources to begin one without a concrete reason. Schultz (2004, page 1) cites the Gartner Group statement that "nothing in the practice of information security produces as much return on investment (ROI) as security training and awareness." Schultz treats this with a healthy amount of skepticism but calls on the research community to examine the issue further. Given their perception as non-critical, training programs are quite vulnerable and having solid evidence to support their critical nature would help bolster their significance. This paper echoes the call of Schultz (2004) to see many more papers on topics related to security training and awareness. This is especially true given that the semantic analysis found this area to be the most pervasive of all the emergent themes.

Resistance to new security measures was the third emergent theme identified. As was previously stated, there is very little security literature to help explore this phenomenon. Furnell, *et al.* (2000) looked into user acceptance of biometrics for authentication. While not looking at policy per se, the authors do illustrate the issue of resistance to security implementation. The opposite of resistance, or acceptance, is described as the friendliness and transparency of the measure and it is difficult to assess, as it represents a highly subjective measure (Furnell, *et al.* 2000). Huston (2001) studied security issues with the implementation of E-Medical records. Again security policy was not at issue but Huston did find that resistance to security devices was apparent. Though vague, a starting point for dealing with resistance was stated as "eliciting the feelings of users concerning their activities and interactions may allow the change agent to positively address areas of resistance." (Huston, 2001, page 94). Although a lot of work has been done in the area of resistance to change (Karahana, Straub, Chervany, 1999; Markus, 1983; Orlikowski, 1993; Baronas and Louis, 1988), there is little work that directly examines how an organization's members might resist security policy implementation. Clearly additional research is needed in this area as well, particularly in the area of security policy.

A lack of specific and well defined socio-organizational controls was the fourth emergent theme identified. This is a still emerging area in the field of security, spearheaded by Dhillon and Backhouse (2000) and integrated into the overall structure of the development of security by Siponen (2001). Four socio-organizational principles are identified by Dhillon *et al.* (2000). These are responsibility, integrity, trust, and ethicality. Responsibility is defined as "not just carrying the can for when something has gone wrong in the past (accountability—for attributing blame) but refers also to handling the development of events in the future in a particular sphere" (Dhillon *et al.*, 2000, page 127). Integrity, or the steadfast adherence to a strict moral code, can be strengthened informally secure arrangements. Trust for and within the members of an organization encompasses personal confidentiality and is reinforced by face to face contact. Ethicality, as it relates to informal norms and behavior, is introduced by the very culture of the organization. Using each of these four areas, a policy formulator can drill down and determine specific issues that can be and should be addressed by a given organization. The ad hoc, reactionary, and vague measures present in the artifact studied for this research show no such analysis.

The final emergent theme identified was the absence of an effective deterrent. The fact that students continuously downloaded copyrighted material demonstrates that the consequences to their actions did not preclude the students from carrying out those actions. Straub (1990) describes two sub-constructs to deterrence: certainty of sanction and severity of sanction. Both of these sub-constructs are called into question in this scenario. Not only are the majority of users unaware of the policy (removing any certainty of sanction unless they are repeat offenders) but when they are sanctioned, the punishment is nominal. It is reasonable to assume that if students were expelled from the University or even just lost network connectivity permanently, the copyright violation policy abuse would drop dramatically. Straub (1990, page 21) found that effective "IS deterrents result in reduced incidence of computer abuse." Given his findings, Straub (1990) calls for detailed security policy, the enlightenment and education of users to the policy, and effective technical controls.

CONCLUSION

The purpose of this study was to establish that a disconnect between security policy formulation and implementation exists. The problem that results from this situation is an ineffective security policy and thus a vulnerable system. In order to examine the phenomena, we created a semantic framework which was based in the theoretical work of Morris (1970), Stamper (1973), and Katz (1970). This framework guided our collection of data and gave a structure for analyzing the data.

The "snapshot in time" of the lifecycle of security policy at the organization under study demonstrated that a disconnect is glaringly evident between security policy formulation and implementation. Not only were most users unaware of the existence of a security policy, but the makers of the policy were not aware of this ignorance. They did not have an opportunity to be a part of the process evolving and developing this document into an optimized form. There also was no guidance available for the formulation policy itself. Some security measures were met with stiff resistance from the user base. Socio-organizational controls were vague and ill described in the policy artifact. Finally, the sanctions to non-compliance tended to be so underwhelming that the consequence became irrelevant. The result of all of this is that you have an organization that has a chaotic and unordered security environment. The security policy artifact is far from a connecting entity between the two sides that should interact with it. The plethora of security incidents cited by the interviewees could be drastically contained and controlled if this disconnect could be patched.

Further research is needed to determine situation within more controlled environments, such as commercial or private organizations. Being a state educational entity may have distorted the results to a degree and having additional, more diverse data would validate the framework to a greater level. Also, this study focused on the relatively small subset of those most directly involved in policy. A quantitative examination of a wide base of users might shed some additional light on policy implementation.

REFERENCES

1. Ahmad, A. and Ruighavar, A. (2003). Improved Event Logging for security and Forensics: developing audit management infrastructure requirements. *The Security Conference*, Las Vegas, NV
2. Anderson, P. (1990). A Theory of Computer Semiotics: Semiotic Approaches to Construction and Assessment of Computer Systems. *Computational Linguistics*. 18(4). pp. 555-562
3. Backhouse, J. Dhillon, G. (1996). Structures of Responsibility and Security of Information Systems. *European Journal of Information Systems*. 5(1). pp. 2-9.
4. Barley, S. (1983) "Semiotics and the Study of Occupational and Organizational Cultures," *Administrative Science Quarterly* (28). pp. 393-413
5. Baronas, A. and Louis, M. (1988). Restoring a Sense of Control during Implementation: How User Involvement Leads to System Acceptance. *MIS Quarterly*. 12(1). pp. 111-124.
6. Baskerville, R. Siponen, M. (2002) An Information Security Meta-policy for Emergent Organizations. *Logistic Information Management*. Vol. 15, No. 5/6.
7. Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys*, 25(4).
8. Coyne, J. and Kluksdahl, N. (1994). "Mainstreaming" Automated Information Systems Security Engineering (A Case Study in Security Run Amok). *ACM Conference (CCS 11/94)* Fairfax, VA
9. Cosgrove, L. (2004). The State of Information Security, 2004. *CIO Magazine and PricewaterhouseCoopers* http://www2.cio.com/research/surveyreport.cfm?id=75
10. Dhillon, G. Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*. Vol. 43. No. 7
11. Furnell, S. Dowland, P. Illingworth, H. Reynolds, P. Authentication and Supervision: A Survey of User Attitudes. *Computers & Security*. Vol. 19. 529-539
12. Glasgow, J. Macewen, G. (1992) A Logic for Reasoning about Security. *ACM Transactions on Computer Systems*. 10(3). pp 226-264
13. Huston, T. (2001). Security Issues for Implementation of E-Medical Records. *Communications of the ACM*. 44(9).
14. Joshi, J. Ghafoor, A. Spafford E. (2001) Digital Government Security Infrastructure Design Challenges. *Computer*. February.
15. Karahana, E. Straub, D. Chervany, N. (1999) Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. *MIS Quarterly*. 23(2). pp. 183-213
16. Katz, J. (1970). Semantic Theory. New York: Harper and Row.
17. Kühnhauser, W. (1999). Policy Groups. *Computers & Security* 18(4) pp 351-363.

18. Markus, ML. (1983) Power, Politics, and MIS Implementation. *Communications of the ACM*. 26(6). pp. 430-444.
19. Morris, C. (1970). Foundations of the Unity Of Science: Toward an International Encyclopedia of Unified Science. Chicago: University of Chicago Press.
20. Orlikowski, W. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly*, 17(3). pp. 309-340.
21. Rees, J. Subhajyoti, B. Spafford, E. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM*. 46(7).
22. Schultz, E. (2004). Security training and awareness fitting a square peg in a round hole. *Computers & Security*. 23(1).
23. Siponen, M. (2001). An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In: Information Security Management: Global Challenges in the New Millennium. Ed. Dhillon, Hershey: Idea Group.
24. Stamper, R. (1973). Information in Business and Administrative Systems. New York: Halstead Press.
25. Straub, D. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*. 1(3). pp. 255-276.
26. Trompeter, C. Eloff, J. (2001). A Framework for the Implementation of Socio-ethical Controls in Information Security. *Computers & Security*. 20(5). pp. 384-391
27. Ulrich, W. (2001). A Philosophical Staircase for Information Systems Definition, Design, and Development. *Journal of Information Technology Theory and Application.* (3). pp. 55-84.
28. Walsham, G. (1993) Interpreting Information Systems in Organizations, Wiley, Chichester, UK.
29. Willison R. (2002). Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank. Dissertation for partial fulfillment of PhD. Department of IS, London School of Economics.