2008

# Power Relationships in Information Systems Security Policy Formulation and Implementation

Michael Stephen Lapke
*Virginia Commonwealth University*

# POWER RELATIONSHIPS IN INFORMATION SYSTEMS SECURITY POLICY FORMULATION AND IMPLEMENTATION

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

By

Michael Stephen Lapke
MS, Computer and Information Systems, University of North Florida
BS, Information Systems, University of North Florida

Director: Dr. Gurpreet Dhillon
Department of Information Systems

Virginia Commonwealth University
Richmond, Virginia

05/2008

# Acknowledgment

I would first like to thank my wife, Shalyn, for the incredible support she gave me during this quest. This support came through a storm of events in which Sha demonstrated her infinite strength and persistence. She endured moving away from her family and into a dark and depressing basement. This continued through the events of Hurricane Isabelle where we lived without power for 20 days. She even went so far as to literally carry me when I ruptured my patellar tendon in the summer of our third year. Before and after the reconstructive surgery, I didn't have the strength to lift my leg and Sha was always there for me. Through it all, she steadfastly endured through her own PhD program. She never surrendered to the pressures of her program and yet still found the time to be there for me. I am especially privileged in that she not only gave me unwavering emotional support and boundless love but she also provided intellectual and spiritual support as well. In these years of tribulation, I knew I had the most beautiful and brilliant woman to come home to and that always gave me the strength to continue. Whether it was a loving embrace or a fellow intellect to bounce ideas off of, Sha was my one constant. For that, I am forever grateful.

It was also through Sha that my greatest inspiration came into the world: my wonderful little boy, Charles Joseph. Every day we spend with CJ has been part of an incredible journey of exploration and discovery. I never knew I could adore something so completely yet each day my love grows. From the first day I held him to the day he first smiled at me to watching his amazing personality emerge each day, CJ has been the light of my life. CJ's little personality and sense of humor (even at 11 months old) makes this world so full of life and joy for me.

Of course, my dissertation would not have been possible without the ever patient guidance of my chair, Dr. Dhillon. His constant presence in my five years at Virginia Commonwealth University has been invaluable towards my intellectual growth. Dr. Dhillon also made sure to assist me in the pragmatic aspects of simply making it through the program. Going back to the strategic dichotomy of planned versus emergent strategy, I still wonder whether Dr. Dhillon knew all along where I was headed. During my very first year, I wrote a paper in the Theory of Information class Dr. Dhillon was teaching. He continually prodded me to keep working on the paper well after the class was completed. I did and the paper evolved into a full research project which we published at AMCIS. He then took it a step further and suggested running with the emergent findings for a potential dissertation. I did exactly that and now have completed the work that began three years ago. It seems as though fate drove Dr. Dhillon towards teaching and advising the upcoming generation of scholars. He has a gift of seeing the greater context but still letting his pupil's find the answer using their own devices. Dr Dhillon has helped me surpass my own boundaries.

I would also like to thank my committee, Doctors Weistroffer, Redmond, Norman, and Lee for their guidance. A special thank you goes out to Dr. Lee for all of the time he gave me in robust philosophical and methodological debate. He opened my eyes and helped me look past the dogma of traditional approaches. I would also like to thank the management at "Millennium Bank" for all their help and exceeding flexibility in opening their organization for my research.  Finally, I would like to thank my mom and dad for giving Sha and I a place to escape in beautiful Virginia Beach and for all their help when CJ was born.  Also, a thank you goes out to my brothers for keeping me sane during my tenure at VCU. To John, I thank you for convincing me to hit the surf and to my brother Paul, I thank you for the all the nights out at the movies.

# Table of Contents

## List of Tables

## List of Figures

# Abstract

POWER RELATIONSHIPS IN INFORMATION SYSTEMS SECURITY POLICY FORMULATION AND IMPLEMENTATION

By: Michael Stephen Lapke, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University.

Virginia Commonwealth University, 2008

Director: Dr. Gurpreet Dhillon
Department of Information Systems

This thesis argues that organizational power impacts the development and implementation of Information Systems (IS) Security policy. The motivation for this research stems from the continuing concern of ineffective security in organizations, leading to significant monetary losses. IS researchers have contended that ineffective IS Security policy is a precursor to ineffective IS Security (Loch et al. 1992; Whitman et al. 2001; David 2002; Solms and Solms 2004). Beyond this pragmatic aspect, there is a gap in the literature concerning power relationships and IS Security policy. This research intends to bridge the gap. The dissertation is a two phased study whereby the first phase seeks to understand the intricacies of IS Security policy formulation and implementation. In the first phase, a conceptual framework utilizes Katz's (1970) semantic theory. The conceptual framework provides the theoretical foundation for a case study that takes place at an educational institution's Information Technology (IT) Department. In the results, it is confirmed that a disconnect exists between IS Security policy formulation and implementation. Furthermore, a significant emergent finding indicates that power relationships have a direct impact on this observed disconnect. The second phase takes place as an in depth case study at the IT department within a large financial organization. The theoretical foundation for the second phase is based was Clegg's (2002) Circuits of Power. A conceptual framework for this phase utilizes this theory. This framework guides the study of power relationships and how they might affect the formulation and implementation of IS Security policy in this organization. The case study demonstrates that power relationships have a clear impact on the formulation and implementation of IS security policy. Though there is a strong security culture at the organization and a well defined set of processes, an improvement in the process and ensuing security culture is possible by accounting for the effect of power relationships.

# CHAPTER 1 Introduction

## 1.1 Scope of the Research

An organization's Information Systems (IS) Security policy is of core importance to an organization's overall IS Security (Hone and Eloff 2002). This is a result of an IS Security policy's indication of management's commitment to and support of IS security, as well as defining the role security has to play in reaching and supporting the organization's vision (Willison 2002). Besides this clarification of the security role, an IS Security policy also provides an anchoring point and proof of high level management's obligation to optimal IS Security within an organization (Solms and Solms 2004). Without this anchoring point, security projects and efforts "will be floundering around without really making progress" (Solms and Solms 2004, pg. 374).

While there is not much empirical research that addresses the result of non-compliance to IS Security policy (Doherty and Fulford 2005), the logical inference (Solms and Solms 2004) is that non-compliance would lead to the security of an organization being questionable. While not directly addressing the question of the extent to which a security policy affects actual security, research has shown its presence is important in reducing security breaches (Loch et al. 1992; Whitman et al. 2001; David 2002; Solms and Solms 2004).

The motivation for this research stems from a long standing and well known issue in IS Security literature: organizations continue to lose substantial sums to failures of IS

Security. According to the most recent FBI/CSI survey (Gordon et al. 2006), more than 52 million dollars was lost in 2006, according to the 313 respondents to the survey. If one extrapolates this figure to all organizations, the monetary losses would be exceptional. Furthermore, 68% of the respondents reported that a portion of these losses was a result of insider threats. An "insider" is defined as employees, contractors and consultants, temporary helpers, and personnel from third-party business partners and their contractors and consultants (Schultz 2002). Almost one in ten reported that an overwhelming majority, 80 to 100%, of the losses were a result of insider threats. This evidence supports the claim that many breaches of information systems in organizations are carried out by insiders (Schultz 2002). It is these insiders that are most affected by IS Security policy. As they are subject to the consequences outlined in the policy as well as the security culture indoctrinated by the policy, insiders are tied to their organization's policy much closer than an outsider.

The presence of a "perfect" IS Security policy would not ensure that an organization is completely protected from these insider threats. An analogy to a perfect IS Security Policy can be seen prisons. Maintaining an air of perfect security is a constant goal within this context. The panopticon metaphor (Silva 1997) was devised by the British philosopher Jeremy Bentham in the late eighteenth century. This was a prison design that consisted of a central tower that was surrounded by a ring shaped building. This allowed for continuous observation of the inmates with minimal resources allocated to the supervision of the inmates. Foucault (1977) extended the concept as a metaphor for modern disciplinary societies and its pervasive inclination to observe and normalize.

The panopticon metaphor was adopted to study Information Technology (IT) implementation (Zuboff 1989; Silva 1997). It was re-branded the electronic panopticon and organizations with an electronic panopticon in place would not tolerate an authoritarian style of management. Silva (1997) states that discipline power works when individuals know that they are under surveillance and once they know how to break the system, discipline will end. Thus, from an emergent perspective (Mintzberg et al. 2003), a perfect IS Security Policy leading to impervious security is an unattainable goal.

While IS Security policy can be seen as a tangible instantiation of discipline, its success is subject to the social reality in a given organization. As noted by Silva (1997), once individuals know how to "break the system," the system becomes ineffective. The social reality this research is focusing on is power relationships. Analyzing the power relationships in an organization during the formulation and implementation of an IS Security policy is hoped to provide a better understanding of how existing power relationships affect IS Security policy.

This introductory section presents a foundation of IS Security policy's place in contemporary organizations. This research seeks to better understand the sociological processes that impact IS Security policy formulation and implementation. The underlying social dynamics that affect the creation and implementation of IS Security Policy are complex and currently ill-defined. Through in depth case study, this research aims to provide a structured analysis of these social dynamics, particularly as they relate to power relationships.

The remainder of this chapter will describe what this dissertation will do in regards to analyzing power relationships in IS Security policy formulation and implementation. The immediate point to be answered, in the following section, is what is the central argument of the dissertation? Following this section, the nature of the research will be addressed. The nature of the research provides definitions to key concepts as well as the theoretical foundation that the dissertation will be based. It will also address the specific research questions that will be answered in the dissertation. The final major section of this chapter covers the contributions, how the study was conducted, and the boundaries of the study.

## 1.2 Argument

This research argues that organizational power impacts the development and implementation of IS Security policy. This relationship is bi-directional in nature. This means that organizational power can affect how IS Security policy is conceived and implemented and IS Security policy can affect organizational relationships and interactions. Of particular interest in this argument is how the power relationships that affect IS Security policy can lead to resistance.

Clegg’s construct of episodic power (Clegg 2002) can illustrate the causal relationship between power structures and resistance. Episodic power refers to the day-to-day interaction, work, and outcomes. One-to-one communication and conflict and their consequences are part of the first of three levels in Clegg’s circuits of power. It essentially acts as a generator of data about power that informs the higher, macro, levels. At this level we see the "intermittent exercise of power" (Clegg 2002, page 187). Since "power always involves power over another, and thus at least two agencies, episodic power will usually call forth resistance because of the power/knowledge nature of agency" (Clegg 2002, page 208).

This argument is based on the complex construct of "power," thus some critical steps must be taken to substantiate the argument. It is noted that IS Security literature exists that deals with other aspects that might affect IS Security policy implementation (Straub 1990; Siponen 2000; Willison 2002; Karyda et al. 2005). It is also noted that there exists IS literature that discusses power and resistance (Markus 1983; Orlikowski 1993). However, this is beyond the scope of this chapter and will be discussed in the literature review.

Preliminary analysis regarding the viability of the relationship between power and IS Security policy formulation and implementation is conducted in the first phase of the research. While the second chapter is devoted to discussing the details of this, a brief overview of the phase is provided. The purpose of the first phase is to understand the intricacies of IS Security policy formulation and implementation. The meanings the stakeholders attribute to the IS Security policy formulation and implementation process are analyzed as a main goal of the first phase. Several emergent themes are identified during this analysis, including lack IS Security policy awareness, lack of IS Security policy strategy, resistance to IS Security policy implementation, and lack of adequate deterrence to non-compliance.

The first phase demonstrates that there is a disconnect between the creation and deployment of IS Security policy. It also finds that power relationships play a part in the problem. Furthermore, during the course of the analysis of the findings of the first case, it is found that very little literature directly addresses power and IS Security policy formulation and implementation. Substantial work had been completed in the other areas but there was limited research that dealt with power and IS Security policy formulation and implementation. As power has not been at the forefront of IS Security policy research, it is important to discuss how other IS researchers have attempted to analyze IS Security Policy. This topic is addressed in chapter three and will demonstrate that a gap in the literature exists regarding power relationships and IS Security policy implementation.

### 1.3 Nature of the Dissertation

This section is divided into five subsections. The first four sections argue definitions for the concepts inherent to the dissertation. The definitions include the foundational constructs of Information Systems (IS), IS Security, IS Security Policy, and power. It is important to thoroughly substantiate these foundational constructs so ambiguity can be avoided. The fifth subsection discusses the specific research questions that this study seeks to answer during the course of the analysis. These questions outline in a more specific fashion what exactly this research is intending to explore.

#### 1.3.1 Information Systems

There are several perspectives regarding how the concept of an IS should be defined. Many undergraduate text books portray the simplistic view that an IS consists of the Information Technology (IT) and the people who use the IT. An IS has been defined as the emergent result of the mutually transformational interactions between the IT and the organization (Stamper 1973; Land 1976; Lee 2004). In other words, once the technical systems are implemented, the IT itself triggers new and different organizational changes. Once these changes are implemented, the new organizational realities require a change of the IT and thus the cycle continues. It is key to differentiate between an IT and an IS in this perspective.

IS has also been defined as a social system that that has been technically implemented (Hirschheim et al. 1995). This is a slight step away from the mutually transformative description in that the focus is on the social or organizational element. A major break in perspectives is that this allows for an IS to exist regardless of the existence of an IT, in the contemporary sense. For example, a "social system" or Universe of Discourse (UoD), could consist of two people speaking. Technically implemented, this could take the form of a piece of paper passed between the two, smoke signals from distant mountain tops, or an electronic encoding of mutually understood characters. This technology makes up the core of the IS and is surrounded by the formal aspects of the social system.

Perhaps a convergence of these definitions could provide the best perspective for defining an IS. The mutually transformative view (Lee 2004)covers the prescriptive side of the definition while the technical implementation of a social system (Hirschheim et al. 1995) covers the descriptive side. While the mutually transformational interactions define what will happen to an IS during its lifespan, it does not lucidly describe a snapshot in time of an IS. Seeing an IS as a technical implementation of a social system provides a rich picture of what an IS should be defined as. It is necessary however to part the technical system from the social system.  While it is an instantiation of a social system, the technical implementation is in fact a separate artifact.  This also utilizes the mutually transformational interactions.

### 1.3.2 IS Security

IS Security has traditionally been dominated by a technically oriented perspective where data confidentiality, data integrity, and data availability (CIA) are touted as the tenets of IS security (Pfleeger 1999; Rogers 2004). Data confidentiality refers to the assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data is not handled in a manner adequate to safeguard the secrecy of the information concerned.   Data integrity refers to the assurance that the information is authentic and complete. In other words, can the information be relied upon to be sufficiently accurate for its purpose?  Data availability refers to the assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Though not a new concept, CIA is still widely used as the way by which security is defined.  The Carnegie Mellon Software Engineering Institute (CERT), a center of Internet security expertise, proclaims that one of the principles of survivability and information assurance is that everything is data (Rogers 2004).  With this said, the point is made that “there are three attributes of data (often referred to as the IS Security triad) that should be considered and secured: confidentiality, integrity, and availability” (Rogers 2004, pg 2).  This statement is supported by a reference to The Committee on National Security Systems (CNSS).

The CNSS was created Under Executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age. The President of the United States redesignated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS). The CNSS defines IS Security as:

> "The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats" (Rogers 2004, pg 3).

This shows a reliance on the CIA principle. Unauthorized access refers to confidentiality, modification refers to integrity, and protection against denial of service refers to availability. The CNSS (Pfleeger 1999) claims that IS Security is solely described with CIA. This perspective is continued by asserting that security consists of maintaining three characteristics: confidentiality, integrity, and availability (Pfleeger 1999).

Dhillon (2007) incorporates technical, formal, and informal aspects of IS Security in providing principles of IS Security. Within the technical aspects, the principles of emergent strategy and micromanagement of CIA are necessary. The first principle, emergent strategy in the management of the security of technical systems, is called for because rationally planned strategies fail when faced with the ground realities (Mintzberg 1983). The second principle, micromanagement for achieving CIA, is critical due to the fact that technical security can only be achieved if the CIA aspects have been completely understood (Dhillon 2007).

Within the formal realm, Dhillon (2007) describes two principles: establishing a boundary between the formal and informal and contextualizing the rules for the management of IS Security. The informal aspects of IS Security include two principles: developing a security culture and making Responsibility, Integrity, Trust, and Ethicality (RITE) the cornerstones of maintaining a secure environment. This layered approach to security, which integrates the technical, formal, and informal, is the most thorough perspective on the genre.

### 1.3.3 IS Security Policy

An IS Security Policy can be defined in different ways, depending on the degree of abstraction taken. Literally, it is a tangible artifact that typically is printed on paper or published electronically. It defines how the confidentiality, integrity, and availability of IS assets are protected (Carroll 1996). The ultimate aim of any computer security policy must be to protect the confidentiality, integrity, and availability of the electronic data held within the system (Loch et al. 1992). IS Security policy has also been defined as the set of laws, rules, and practices regulating how an organization manages, protects, and distributes sensitive information (Whitman et al. 2001).

At a higher level of abstraction, IS Security Policy can be seen as a component of an organization's IS Security Strategy. This view of policies places them in the grander scheme of the overall strategic process. This being that a strategy is a pattern that integrates an organization's objectives, policies, and action sequences (Mintzberg et al. 2003). This conceptualizes an IS Security policy as "a wide ranging document which is about managing the business as a whole, managing it securely and protecting a company's key asset: its information" (Whitman et al. 2001, pg. 10).

### 1.3.4 Power

The Oxford English Dictionary (OED) defines power in several different ways including "the ability or capacity to perform or act effectively" and "the ability or official capacity to exercise control; authority." Although these definitions are accurate depictions of power, they fall short of the richness of what the concept is, along the lines of the sociological debates of power. Silva provides a typology of power that addresses this concern (Silva 1997).

Silva's typology consisted of four dimensions of power, including *power to*, *power over*, *power storage*, and *power discretion* (Silva 1997). 'Power to' is power that enables an individual to act. This has been articulated in the IS literature by a proposal for an emancipatory IS development (ISD) methodology (Hirschheim and Klein 1994). Emancipation refers to freeing individuals and groups from repressive social and ideological conditions that hinder human communication. The methodology, Effective Technical and Human Implementation of Computer-based Systems (ETHICS), (Mumford 1983; Hirschheim and Klein 1994) offered an approach to ISD that allowed for communication acts that were free from power and authority.

'Power over' mirrors the second definition described in the OED. This is the ability of a group or individual to exercise influence over another group or individual, particularly if this is in a manner that is contrary to the latter group's interests. This type of power has been explored in the IS literature in light of the implementation of an IS

(Keen 1981; Markus 1983; Orlikowski 1993). Orlikowski (1993) sought to determine whether IT determined organizational change or if the organization determined the IT itself. Keen (1981) and Markus (1983) both considered resistance exerted by users to the implementation of an IS.

'Power storage' refers to the bureaucratic and institutional forces maintaining a power relationship over a time period. This could be described with a military analogy (Silva 1997). The ongoing and standing disciplinary power a general holds over his subordinates is a clear example of power storage. In the IS literature, this is seen in work that examines resource dependency as well as contingency theories.

'Power discretion' describes the options that agents have in hand to deploy the power that is stored. An agent can switch 'power to' or 'power over' on or off. Silva notes that research in IS that is influenced by the 'power discretion' aspect of power is concentrated on the relationship between decision making and power (Silva 1997). This is particularly the case with the political nature of decision making.

### 1.3.5 Research Questions

The argument behind this research is that the introduction or modification of an organization's IS Security policy can have an impact on existing power relationships within the organization. This impact can lead to non-compliance or an ineffective IS Security policy. The aim of the research is to investigate how power relationships within an organization are affected by the formulation and implementation of IS Security Policy as well as how the formulation and implementation of IS Security Policy is affected by the power relationships. The research also seeks to investigate how the formulation and implementation of IS Security Policy is affected by the power relationships within an organization.

The focus of the research leads to the following research questions:

1. In what ways do power relationships within an organization have an impact on the formulation of IS Security policy?
2. In what ways do power relationships within an organization have an impact on the implementation of IS Security policy?
3. To what degree does the implementation of an IS Security policy have an impact on the existing power relationships within an organization?

## 1.4 Conclusion

This study intends to fulfill several goals. A primary goal involves the creation of new theoretical models that aim to illustrate the relationship between organizational power and IS Security Policy. Another goal involves filling a gap in the extant literature. This contribution consists of adapting and interpreting Clegg's Circuits of Power theory (Clegg 2002) to the study of IS Security. There is very little research that investigates power and resistance to IS Security policy implementation. Secondly, at a practical level, having a better understanding of the social implications of formulating and implementing IS Security policy can lead towards an IS Security version of Zuboff's (1989) utopian vision of IT. This vision sees more interaction between managers and subordinates and mutual influence between once adversarial agents.

This chapter presents the foundation for the research. The first section, the scope, discusses the rationale behind the research. The argument is discussed in the second section. It is argued that power relationships within the organization impact the development or implementation of an organization's IS Security policy. The nature of the research follows the presentation of the argument. This includes defining key concepts as well as providing detailed research questions that this dissertation answers.

The following paragraph outlines the structure of the dissertation and gives a brief synopsis of each of the remaining chapters. The dissertation is divided into seven chapters. The first introduces and discusses what the researcher is studying in the dissertation. The second chapter details the first phase that substantiates the proposed area of study. The third chapter is the literature review and gives an overview of the supporting literature in the areas of IS policy and IS Security policy. The fourth chapter is the theory and methodology chapter and provides evaluation criteria for the methodology. Data collection methods and the mode of analysis are also discussed. The fifth chapter discusses the actual study including the background of the site, the security policy of the site, and the culture and organization of the site. It also reviews the findings of the study. The sixth chapter analyzes and synthesizes the basic findings discussed in the fifth chapter. The seventh and final chapter provides the conclusion to the study and includes a review of the findings and analysis, a discussion of the contributions of the dissertation, a discussion of the potential criticisms, and potential future research directions.

# CHAPTER 2 Phase One: Omega University

## 2.1 Introduction

The first phase seeks to understand the intricacies of IS Security policy formulation and implementation. The motivation of this initial study is exploratory in nature and has layered goals and expectations. The explicit, overlying intent of this first case is to discover whether a disconnect exists between IS Security policy formulation and implementation. Better understanding the sociological intricacies that drive these processes is hoped to lead to identifying the themes that partake in the disconnect.

This disconnect can lead to a failure of the policy. What a stakeholder may have intended to be implemented could be written to imply a different intention within a policy. The intent could also be inferred to mean something different by a stakeholder. Either or both of these potential scenarios can lead to a disconnect between IS Security Policy formulation and IS Security Policy implementation. In practical terms, one such scenario could manifest itself in terms of a policy board creating vague policy that does not explicitly address the pertinent issues. Another instantiation of a scenario could be seen by a user interpreting a "robust" password policy to mean that they should keep track of their changing passwords via a list taped to their monitor.

This chapter is organized into five sections, not including the introduction section. The first discusses the theoretical foundation and will lay the groundwork for the conceptual framework that was used in this first case. A short section on the methodology follows the theoretical foundation section. Given the similarity on methodologies used for the first and second phases, the brevity in this section will avoid potentially redundant information being presented. The case study, including exemplars of actual data, will be contained in a section following the methodology. This section also has four subsections which correlate to the four dimensions of the conceptual framework. A synthesis section, titled "discussion," follows the case study section. This section presents the interpretation of the analysis of the data. The final section concludes the first phase and summarizes the findings.

## 2.2 Theoretical Foundation

Given the exploratory nature of this case and the fact that stakeholder interpretations are being extrapolated, a theory that focuses on "meaning" is most appropriate. Semantic theory, (Katz 1970; Stamper 1973) is the essence of analyzing the meaning of information. With semantic theory, a researcher can understand the meanings attributed to the item of study by the stakeholders.

Semantic theory is a subset of semiotic theory. Semiotics is the science of sign systems including linguistics, as well as the study of all other sign systems (Anderson 1990). A sign is any element that is used to carry information such as a mark on a piece of paper, an electronic bit on a circuit board, or compressed air in the form of sound waves. 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 (Stamper 1973; Anderson 1990; Liebenau and Backhouse 1990; Backhouse 1992; Ulrich 2001; Dhillon and May 2006).

Stamper presents a framework for semiotics that breaks down information into four different "levels" (Stamper 1973). These are empirics, syntactics, semantics and pragmatics. They represent a spectrum of information that moves from the natural world to the social. Semantics is representative of the *meanings* of signs. This concise and elegantly simple semantic model, part of the overall semiotic model, is one that can be used to build a framework in which all dimensions of meaning can be explained (Stamper 1973).

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

The second semantic element, affective descriptions are those that are more based on subjective feelings and human values. They are described as "value judgments: reports on staff, estimates of the relative difficulties of jobs" (Stamper 1973, pg 75). A key, distinguishing, characteristic of affective information is the reference to individual human feelings. Credence is given to this subset of semantics in 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” (Stamper 1973, pg 75). Affective descriptions have also been described as the way in which the actor transfers his choice of an impulse-satisfying object from the consummation phase to the orientation phase (Morris 1970).

A new area is uncovered in the third semantic element, denotative prescriptions. The first two elements deal with how a sign is described. Denotative prescriptions and affective prescriptions differ from descriptions in that they are directive. These are described as “an order, a rule or a recommendation that will denote the objects to which the prescribed action must be related” (Stamper 1973, pg 77). Morris 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 (Morris 1970). 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, pg 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 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, pg 77).

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 IS security policy formulation. This semantic framework is presented in Table 2.1.

| **Semantic Element** | **Description and seminal works** | **IS Security Policy Formulation** | **IS Security Policy Implementation** |
|---|---|---|---|
| Denotative Descriptions<br>• Designation<br>• Facts<br>• Evidence<br>• Forecasts | This semantic element is simply a statement of something that exists. (Stamper, 1973)<br>The nature of the environment in which the organism operates. (Morris, 1970). | What are the known current vulnerabilities of the system in question?<br>How technically secure is the IS in its current state?<br>How physically (and socially) secure is the IS in its current state?<br>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?<br>Is the security policy required reading for all the users of the system?<br>Are the security policy procedures actually followed by the IS users? |
| Affective Descriptions<br>• Appraisals<br>• Value<br>• Judgments | Value judgments: reports on staff, estimates of the relative difficulties of jobs. (Stamper, 1973)<br>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?<br>Do the IS users feel that the current level of security is acceptable?<br>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?<br>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<br>• Instructions<br>• Plans<br>• Policies<br>• Orders | An order, a rule or a recommendation that will denote the objects to which the prescribed action must be related. (Stamper, 1973)<br>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?<br>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 of technical security?<br>Are IS users aware of the specific security policies in terms of the social aspects of security? |
| Affective Prescriptives<br>• Inducements<br>• Coercion<br>• Threats<br>• 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?<br>How much of a burden is security policy enforcement? | Have any personnel that have broken security policy actually been punished?<br>If they have been punished, are any of them repeat-offenders? |

**Table 2.1: Conceptual Framework for Semantic Analysis**

## 2.3 Methodology

The first phase is conducted via an interpretive case study in the Information Technology Department of "Omega University" (the name has been changed to protect the identity of the organization). The term "interpretive" follows the perspective of Walsham who states that our knowledge of reality is a social construction by human actors (Walsham 1993). This knowledge of reality applies equally to researchers and leads to the fact that "there is no objective reality which can be discovered by researchers and replicated by others, in contrast to the assumptions of positivist science" (Walsham 1993, pg 5). This perspective was echoed by Howcroft and Trauth who state that "interpretive researchers aim to develop idiographic theories pertaining to individuals in specific social settings and time periods" (Howcroft and Trauth 2005, pg 33). In other words, "Interpretive research provides in depth insights into social, cultural and historical contexts within which particular events and actions are described and interpreted as grounded in the authentic experiences of the people studied" (Howcroft and Trauth 2005, pg 33).

Approximately two dozen employees work for the department under study. Data was gathered by way of semi-structured interviews. The subjects are the stakeholders involved in the formulation of the IS Security Policy. The interviews are grounded by the conceptual framework. The framework provides a structured foundation for the interviews but there was an open end to the interviews as well. The term structured refers to the interviews being guided by a set of framework-prepared questions. The open-ended aspect occurs 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” helps clarify the researcher’s interpretations and deepen his level of understanding (Walsham 1993).

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

Once the interview process is complete, the data is 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. These thematic principles, which included such topics as security awareness, deterrence, and resistance, emerged in part from existing themes in the security literature and by the data gathered in the course of the study. The result of this process is explored in the Discussion section.

### 2.4 Phase 1 Case Study

This phase of the research takes place at Omega University over the course of a one year period between the summers of 2005 and 2006. The recruitment strategy involves fostering a research subject 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 IS 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 with approximately 20 hours of interview time. This group of subjects represents virtually all of the people directly or indirectly involved with IS Security Policy formulation and implementation at the site. The discussion of the Case Study section is divided into four subsections which are guided by the semantic framework (table 2.1).

### 2.4.1 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 is relatively straightforward to devise areas of exploration concerning policy. Regarding policy formulation, questions include 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 are as straightforward in content but actually more difficult to answer. These include the following: Is the IS Security Policy in place easily accessible by the users and IS staff? Is the IS security policy required reading for all the users of the system? Are the IS Security Policy procedures actually followed by the IS users?

A member of the “Security Planning Team,” an operating systems analyst, was 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 toward a lack of control over the control itself (Baskerville and Siponen 2002). The perspective is substantiated by the view of an administrative member of the University’s IS security policy advisory board. She stated that “the labs are set up by a staff of students with limited technical skills.” This interpretation is reinforced by a number of relatively serious incidents described by the interviewee. The security officer explained how 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. The security officer cited another example, where users disregard policy by opening executable attachments to email. The consequences to the University network were 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, the Chief Information Officer (CIO) and some of the lower level network administrators provided pertinent information. It is quite surprising that none of the administrators were even aware that a specific IS Security Policy even existed. The CIO 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 but most users wouldn’t know where to start.”

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 IS Security Policy. If the relatively savvy and experienced network administrators ignored this, it is pretty clear that the average user would as well. This lack of awareness (Straub and Welke 1998; Trompeter and Eloff 2001; Willison 2002; Schultz 2004) can significantly lead to an increase in a system’s risk to attack.

### 2.4.2 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 IS security policy is written in simple language that most (non-technical) users could easily understand and whether the procedures detailed in the IS security policy are ridiculed or readily accepted by the IS users.

The unique environment of the organization, in that it is a state University, affects this area of the semantic analysis. According to the CIO, the sentiment of staff towards the IS security policy "depends on which staff you talk to." A faculty member of the security planning team stated that, in her department,

> "The users are content and aware of the policy but in other departments, people either don't seem like they know about security concerns or don't care about them."

The relationship between decentralized organizations and decentralized IS can be tenuous and ill defined (Olson and Chervaney 1980). It seems though that this attitude reverses quite quickly when additional security measures are suggested. Prior in the case, 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:

> "The email attachment policy 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 CIO 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. We had a situation where we blocked ports for computers that had a web server set up but had not registered the server with us. We had a ton of faculty explode with protest. What is ironic was that ended up making my job harder."

This phenomenon of resistance to IS Security Policy implementation has not been thoroughly explored in security literature. User acceptance towards authentication is one avenue of research that has examined resistance and IS Security (Furnell et al. 2000). Security issues coinciding with the implementation of E-Medical records and how they may be resisted by the user base is another area (Huston 2001). What can be extrapolated from this episode of resistance is that it is indicative of deeper sociological processes, revolving around power relationships. Given the relatively unbounded power status of "faculty" members of this particular organization, this restructuring of power relationships between "faculty" and the "IT department" resulted in a form of resistance. Based on the interviews with the IT personnel, it is apparent that verbal and behavioral resistance was occurring.

### 2.4.3 Denotative Prescriptions

The next major area of semantic analysis moves away from descriptions and towards prescriptions. The first classification of prescriptions, denotative, is an order, a rule or a recommendation that denotes the objects to which the prescribed action must be related. This is addressed in policy formulation by determining how the current IS Security Policy handles data security issues (confidentiality, data integrity, and availability) and how it handles socially related security issues. These socially related issues have been described as responsibility, integrity, trust, and ethicality (Dhillon and Backhouse 2000). These areas address the soft issues of security that had been ignored for technical issues prior to Dhillon and Backhouse's work. For policy implementation, it should be determined if IS users are aware of the specific security policies in terms of socially related and technically oriented security (Dhillon and Backhouse 2001).

Examination of the IS 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. The areas of responsibility, integrity, trust, and ethicality (Dhillon and Backhouse 2000) are not addressed. 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 (Siponen 2001). This is detrimental because it fails to account for the social dimensions of IS security (Dhillon and Backhouse 2000). 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. None of them were actively aware of an IS security policy, much less of the details of such a policy. This lack of awareness can be detrimental to the overall IS security of the organization (Trompeter and Eloff 2001). They demonstrated that there is an acute need for creating and heightening socio-ethical information security awareness.

### 2.4.4 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 section. On the policy formulation side, this can be answered by determining if the consequences for non-conformation to the IS 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 IS 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).

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 IS Security Policy is a challenging task. Coming up with good and effective policy is critical though. This is discussed in the following section.

### 2.5 Discussion

In the analysis of the case study data, five emergent themes are identified. These themes clearly have a significant impact on the hypothesized disconnect between IS Security Policy formulation and IS Security Policy implementation. The denotative descriptions phase of semantic analysis reveals the organization has 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 and Siponen (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 and Siponen 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 and Siponen 2002, pg 8). The final imperative, criterion-oriented, is described as the policy makers demonstrating an explicit focus on the priorities of the organization. Enacting a meta-policy could alleviate the ambiguity demonstrated by the makers of the IS Security Policy at this particular organization (Baskerville and Siponen 2002).

The most frequently occurring theme appeared during the investigation of the denotative description, affective description, and denotative prescription areas of semantic analysis. This is the issue of lack of awareness of the IS Security Policy. This is not a problem unique to this organization as the 1998 NCC Business Information Survey finds that only one third of organizations provided any form of security awareness training (Willison 2002). Furthermore, "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, pg. 124).

There exists an acute need for creating and heightening socio-ethical information security awareness (Trompeter and Eloff 2001). “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” (Trompeter and Eloff 2001, pg 386). This can be best done through education and awareness programs (Trompeter and Eloff 2001). 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. The Gartner Group states that “nothing in the practice of information security produces as much return on investment (ROI) as security training and awareness” (Schultz 2004, pg 1). 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 findings of this case echoes the call of Schultz to see more research 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.

Changing power relationships, leading to resistance to new security measures is the third emergent theme identified. As was previously stated, there is very little security literature to help explore this phenomenon. The issue has been touched on by Siponen (2001), who stated that resistance may arise from a person seeing certain actions as totally wrong or deficient. Furthermore, he found that if guidelines (which typically take the form of policy) are so weighty and obligatory that they lead to prescriptive states, they can cause greater risks in the form of resistance. Another resistance related area studied examined security issues with the implementation of E-Medical records (Huston

2001). IS 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, pg 94).

Although a lot of work has been done in the area of resistance to change (Markus 1983; Baronas and Louis 1988; Orlikowski 1993; Karahana et al. 1999), there is little work that directly examines how an organization’s members might resist IS Security Policy implementation. With the contention that changing power relationships are the underlying cause to this perceived resistance, this dissertation is laying the groundwork for significant future research.

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 but is gaining traction (Dhillon and Backhouse 2001). It has been integrated into the overall structure of the development of security (Siponen 2001). Four socio-organizational principles have been identified (Dhillon and Backhouse 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 and Backhouse 2000, pg 127). Integrity, or the steadfast adherence to a strict moral code, can be strengthened at an informal level by the use of cultural artifacts within the organization. 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 is 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 found that effective "IS deterrents result in reduced incidence of computer abuse" (Straub 1990, pg 21). Given his findings, Straub (1990)calls for detailed IS Security Policy, the enlightenment and education of users to the policy, and effective technical controls.

## 2.6 Conclusion

The explicit purpose of the first phase is to establish that a disconnect between IS Security Policy formulation and implementation exists. The underlying expectation is to establish how power relationships affect IS Security policy formulation and implementation. In order to examine the phenomena, a conceptual framework, based on the theory of semantics (Katz 1970; Morris 1970; Stamper 1973) is utilized. This framework guides the collection of data and gives a structure for analyzing the data.

The "snapshot in time" of the lifecycle of IS Security Policy at the organization under study demonstrates that a disconnect is evident between IS Security Policy formulation and implementation. Five emergent themes are identified in the analysis of the data collected during the first case study. These include lack of awareness, lack of policy formulation guidelines, vague and ill-defined socio-organizational controls, and ineffective deterrents. The fifth emergent theme identified manifested itself as resistance but has underlying sociological processes, revolving around power relationships. As is discussed in the following chapter, the first four emergent themes have a solid base in the IS Security literature. The fifth emergent theme, which revolves around power relationships, has very little supporting literature in the realm of IS Security. This demonstrates the need for more research of IS Security Policy through the lens of power relationships. It is this fact that is the impetus for the second phase of the research.

# CHAPTER 3 Literature Review

## 3.1 Introduction

This dissertation addresses how power relationships affect the formulation and implementation of IS Security policy. As IS Security policy is a subset of IS policy and IS policy is a subset of general business policy, it is important to establish a baseline review of literature that discusses these supersets. This gives a better contextual understanding of the IS Security policy literature.

Business policy has been conceptualized as an essential element of strategic management (Mintzberg et al. 2003). Two perspectives make up the way in which strategy is made: deliberate formulation and emergent formation (Mintzberg et al. 2003). The classical approach advocated by Quinn (Mintzberg et al. 2003) is the approach to strategy grounded in the military strategy used for thousands of years. This type of strategy advocates the use of deliberate plans to win battles and wars. Noted historical figures in the area of military strategy, such as Sun Tzu, Napoleon, Lenin, and Machiavelli have contributed to advancing the classical strategy to its modern form. Mintzberg (2003)stepped away from this rigid approach to business strategy and policy by advocating an emergent approach. In this, an organization's realized strategy is a combination of deliberate strategy with evolving, emergent strategy. This emergent strategy is identified by a stream of actions which can represent a pattern.

These two perspectives of strategic management can be used to describe the research exploring IS Security policy. One stream is grounded in the classical approach while the other in the emergent approach. The following sections will utilize each of these perspectives in examining the literature behind IS Security policy.

The remainder of the chapter will be organized into four sections. The first of these sections will discuss the literature for business and IS policy, both classical and emergent. The second will review the classical and emergent literature behind IS Security policy. The third section will explore the relationship between the literature supporting business and IS policy and the literature supporting IS Security policy. The fourth section, a discussion section, will analyze where the extant literature leads to with regards to the proposed research in this dissertation. The chapter will conclude with a section recapping the major points of the literature review and providing a prelude to the coming methodology chapter.

### 3.2 Business and IS Policy

Business policy has been defined as a rule for generating action alternatives, for choosing among action alternatives, or for implementing action alternatives (Svenson et al. 1966). It was further described as something that is constant in the short term but changes slowly in the long term. In other words, “policies are rules or guidelines that express the limits within which actions should occur. These rules often take the form of contingent decisions for resolving conflicts among specific objectives” (Mintzberg et al. 2003, pg. 3). This view of policies however does place them in the grander scheme of the overall strategic process. This being that a strategy is a pattern that integrates an organization’s objectives, policies, and action sequences.

It was not until the 1950s that academic interest in business policy began (Leontiades 1982). This was spurred by the new world reality after World War II where companies had to deal with “changing consumer spending patterns, development of new competitive strategies, and the uncertainties of a relatively uncontrolled market place” (Leontiades 1982, pg. 45). The implied need was for long range planning and this was coined as “strategic management.” Strategy is seen as an integral part of defining business policy. One approach to business strategy utilizes four strategy measures along which a firm’s strategy can be parsimoniously captured (Hambrick 1980). They include cost efficiency, asset parsimony, differentiation, and scale.

Another, widely used approach to business strategy is Porter’s (1979) Five Forces Framework. The five forces consist of four forces, bargaining power of customers, the bargaining power of suppliers, the threat of new entrants, and the threat of substitute products, influencing a fifth force, the level of competition in an industry (Porter 1979). Though subject to criticism, Porter’s framework has been a leading force in the area of business strategy.

Moving from business policy to IS policy, one can again approach the issue from a strategic perspective. In the Information Systems Strategy framework (Galliers 1999), IS policy was incorporated along with issues of e-business and knowledge management into the strategic framework. This was substantiated with the contention that “information strategy might also usefully identify information that could question the taken-for-granted assumptions on which the business strategy was based (i.e. as well as providing information to enable the business strategy to be implemented)” (Galliers 1999, pg. 229).

On the alignment track, a call for “electronic business managers and researchers to increase their attention to the emerging policy frontiers and employ theories and methods integrating policy with market and technology issues” (Jarvenpeena and Tiller 1999, pg. 235) was made. This, in essence, is calling for an alignment of Business and IS policy. The concept of business-IS alignment was researched heavily in the 1990s and into the 2000s (Barley 1990; Earl 1993; Venkatraman et al. 1993; Lederer and Salmela 1996; Galliers 1999; Segers and Grover 1999; Reich and Benbasat 2000).

IS alignment refers to “the degree to which the information systems plan reflects the business plan” (King 1978). This alignment could be approached from a socio-organizational perspective where the alignment refers to more of a balancing of the social organizational changes as a result of the IT/IS insertion (Barley 1990). It could also be examined through a managerial lens such as Strategic Information Systems Planning (SISP) (Earl 1993). Four areas of focus in SISP are noted for their presence in the literature: aligning investment in IS with business goals, exploiting IT for competitive advantage, directing efficient and effective management of IS resources, and developing technology policies and architectures.

Segers and Grover (1999) found that SISP effectiveness can be identified by four dimensions. The dimensions they identified are alignment, analysis, cooperation, and improvement in capability. Of these, the key factor identified for successful IS planning is the close linkage of the IS strategy and business strategy. They found that this “alignment helps facilitate acquisition and deployment of information technology that is congruent with the organization's competitive needs rather than existing patterns of usage within the organization" (Segers and Grover 1999, pg. 205).

This focus on strategic alignment was also called for by Lederer and Salmela who offered a theory of SISP (Lederer and Salmela 1996). IS alignment is a critical component of their theory of SISP. Because the successful implementation of the information system is done by aligning the results of the strategic information systems planning process with the business needs of the organization (Lederer and Salmela 1996), alignment is the most important part of their theory. As each of the components in the theory are dependent on the previous component and as alignment is the last component, the theory actually predicts alignment (Lederer and Salmela 1996).

Reich and Benbaset (2000) introduced a model that includes four factors that would influence alignment: shared domain knowledge between business and IT executives, IT implementation success, communication between business and IT execs, and connections between business and IT planning processes. While their findings supported this model, for the most part, an interesting side note that has significant impact on this study came about. This side note had to do with the alignment of business and IS policy (opposed to the generic sort of business and IS/IT alignment), or in Reich and Benbaset's words: "the level of connections between IT and business planning processes" (Reich and Benbasat 2000, pg. 105). This was the one part of their model that was not supported, for either short term alignment or long term alignment.

The terminology and constructs used in the literature can sometimes be murky and vague. When does business strategy end and business policy begin? Where is the line between business and IS? Much of the usage of terms such as IS and IT were intermingled and this does not fit into the definition of IS that was presented in the first chapter. According to that definition, they are not separate constructs. Despite the ambiguity, several themes are apparent in the IS policy literature. Firstly, IS policy is an integral part of strategic IS planning. Second, much of the literature in IS strategy has focused on IS-business strategic alignment. Thus, the implication is that alignment between IS policy and business policy is equally critical.

## 3.3 IS Security Policy

According to Dhillon and Torkzadeh (2006), "In the past most secure system development activities and organizational security policies have been exclusively based on the principles of confidentiality, integrity and availability" (pg. 293). They further indicate that "part of the problem related to our inability to manage and ensure IS security has been our over-reliance on these three issues and simultaneously ignoring the more organizationally based, value measures" (Dhillon and Torkzadeh 2006, pg. 293). This perspective of an IS Security policy techno-centric bias in the literature is supported by the large number of technically oriented articles on topics such as firewalls (Harris and Hunt 1999; Kamara et al. 2003; Wool 2004), intrusion detection (Cho and Park 2003; Han and Cho 2003), internet security (Spinellis et al. 1999), cryptography (Hoffman et al. 1994; Landau et al. 1994; Lin 2001), and access control (Sandhu 1992; Foley 1997; Ward and Smith 2001). This stance is tempered however by the fact that the technical aspects form the core of IS Security, as described by Dhillon (2007). What needs more exploration however are the formal and informal organizational aspects of IS Security.

There has been work though that has focused on the organizationally based IS Security policy issues. Besnard and Arief (2004) examine the cognitive processes behind security lapses whereby the level of protection is traded-off against usability. They recommended that the design of security products and policies should rely more on the rules of human-computer interaction. If they are not, then it is likely that the rules will not be followed. They justify this with the logical conclusion that though it may seem an unworkable view to security officers but the reason why security policies have to be enforced to humans is because these policies require an effort from them. If the rules are felt to be too costly to follow, they are simply respected.

While this view of IS Security Policy is at a high level of abstraction, there is research that looks into specific areas of IS Security policy. Of all of the areas within IS Security policy, formulation is the most vetted and thoroughly discussed genre. It is likely easiest for researchers to determine the best way to plan something instead of putting something into motion.

Both Anderson and Gritzalis examine the role of IS Security policy formulation in the world of health care (Anderson 1996; Gritzalis 1997). This is a pertinent area of research because of the current drive towards the digitization of patient records as well the inherent privacy and confidentiality of those records. Anderson was asked by the British Medical Association (BMA) to create a policy model. Based on military and banking policy models and informed by the clinical expertise of the BMA, Anderson created a descriptive hierarchical policy model designed specifically for health care systems (Anderson 1996). This model is directed towards the formulation of policy for health care IS.

Ferris examined the security policy of the United States Treasury and offered an analysis based through the context of standards (Ferris 1994). Some of the problems he identified were the policy's lack of emphasis on the importance of establishing an information security policy, and that potential IS Security policy issues should be more tractable. On the positive side, the policy mandated the use of ANSI x9.9 standard. The final contention was that IT security standards should serve as the language of Treasury policy decisions. In other words, an integral part of policy formulation should come from the use of standards.

While not focused on a specific industry or area, Trček (2003) offered a framework for IS Security management and policy formulation. As it was related to the entire process of security management, security policy was only a part of this entire framework. For the formulation of security policy, Trček (2003) suggests adhering to the British standard, BS7799. This standard considers an Input – Process – Output model for the creation of security policy. The input consists of legislation, contractual obligations, standards and requirements as the minimal baseline. The first phase of the "process" consists of defining several areas including the security organization, control and assets, physical and environment security, personnel security, access control, and compliance. The second phase of the "process" involves items such as specifying auditing, specifying inter-organizational issues, planning for continuity, and considering privacy. With the input processed, the output is the security policy itself.

The use of standards for IS Security policy formulation has also been looked as a part of Sarbanes-Oxley compliance. The Congress Of The United States passed the Sarbanes-Oxley Act of 2002 (SOX) in response to financial fraud and deception in firms such as Enron, whose public auditing firm failed to discover this abuse (Haworth and Pietron 2006). By bringing an organization towards compliance with the security standards set forth in the International Standards Organization (ISO) 17799, that organization can move towards SOX compliance. The first of the 10 areas addressed in ISO 17799 is security policy. This sets a baseline for IS Security policy formulation whereby the policy should contain references to applicable legislation and regulation. In reference to the IS Security policy formulation articles in SOX, Richard Clarke, former White House advisor for cyberspace security stated:

> "The most important thing a CIO can do to make his or her business safer is clearly articulate an IT security policy, make sure everyone in the organization knows their piece of it, and then enforce it. You can't assume anymore that your system is going to be infallible. And if you throw all of your money into one thing and don't sit back first and de-fine an IT security policy, then you'll probably end up spending your money foolishly" (Damianides 2005, pg. 77).

IS Security policy formulation has also been explored at the theoretical level. One approach to this has been the creation of a formal framework for specifying security policies (Glasgow and Macewen 1992). 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 (Glasgow and Macewen 1992). While not as immediately practical for practitioners, as the government compliance discussed with SOX, it is helpful to expand the theory behind IS Security policy formulation.

Siponen (2001) applied a theoretical perspective to a practical issue. He compared the major IS Security methods: checklists, standards, maturity criteria, risk management, and formal methods. In this comparison, it can be seen that the methods prescribed by the practitioner-oriented papers fell into the first two generations described by Siponen. The "security principles" discussed in the health field (Anderson 1996; Gritzalis 1997) imply a generic checklist (1st generation IS security methods). The BS7799 standard (Trček 2003) is a 2nd generation IS security method in that it is a standard. This theoretical view is important to the analysis of IS security policy formulation because it demonstrates that there exists a continued need for evolution in the IS security methods that IS Security policy formulation resides.

Baskerville and Siponen specifically tackle the issue of policy formulation by way of calling for a security meta-policy (Baskerville and Siponen 2002). 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.

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. Though this is not an explicit meta-policy, it implies a policy about policies in that the proposed framework encapsulates the policy formulation process in a lifecycle.

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

Besides IS Security policy formulation, there’s the aspect of IS Security policy that gets less attention: implementation. While formulation deals with how the policy is made, implementation is concerned with how it is put into use. As a researcher, it is difficult to catch practitioners “in the act,” which is why fewer work has been done.

The work that has been done in IS Security policy implementation studies tends 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 and Kluksdahl 1994). To combat this issue, the authors issue a 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.

Instead of examining a failed IS Security policy implementation for insight (Coyne and Kluksdahl 1994), Trompeter and Eloff (2001) provided a framework for implementation of socio-ethical controls in IS security. While not specifically referring to IS Security policy, socio-ethical controls are closely related. One of Trompeter and Eloff's (2001) points was that people should be placed at the center of the equation, rather than at its periphery. One way to do this is to "adopt an information security policy that includes its viewpoint on socio-ethical IS Security awareness issues. This policy can then be used to guide staff members as to, for example, the various ways in which to protect client information" (Trompeter and Eloff 2001, pg. 387). Though the authors do not go into the mechanics of implementation, their insight is critical because it instantiates the later generations of the analysis of the evolution of IS security methods (Baskerville 1993; Siponen 2001).

Doherty and Fulford (2005) made an unexpected finding when they sought to determine whether IS Security policies reduce the incidence of security breaches. They found no statistically significant relationship between the adoption of IS Security policies and the incidence of security breaches. Though this may seem to be detrimental to the core assumption of this research (that is that it is implied that better understanding policy formulation and implementation will lead to better policy which will then lead to better security), in reality it bolsters the case for the research. The authors speculated as to why this counter-intuitive finding might come from their research. They suggest that difficulties in raising awareness, difficulties of enforcement, too complex policy standards, inadequate resourcing, or failure to tailor policies might be to blame (Doherty and Fulford 2005). These speculations are referenced to IS security literature that finds that they each are indeed problems. This dissertation however specifically tackles the issue of IS Security policy and may be able to help resolve these unexpected findings.

An appropriate parallel to IS Security policy implementation is general IS or Information Technology (IT) implementation. A noted work in the area is Markus' (1983) article on IS implementation. The paper provided grounded starting point for analyzing IS implementation. The main focus was on resistance to IS implementation and how a researcher could study the phenomenon. Cavaye and Chritiansen (1996) extended the work of Markus (1983) and others by presenting a framework to measure subunit power. Cavaye, and Chritiansen (1996) found that the framework was useful for mapping relative power distribution at different moments in time.

Orlikowski (1993) looked specifically into the implementation of an IT in the form of Computer Assisted Software Engineering (CASE) tools. Her contention that the introduction of an IT involves a process of organizational change over time can be used as a parallel to the introduction if an IS Security policy into an organization.

The articles discussed in this section imply a common thread. This thread is that security policy implementation or IS/IT implementation are usually problem ridden. The problems tend to be organizational in nature and can go so far as to cause the failure of the item being implemented. This is not a new concept in IS but to further justify the study in this dissertation, it is an argument that must be clearly stated.

Moving back from non-compliance of IS implementation to non-compliance of IS Security policy, some have approached this from a social-theory perspective. These studies tend to be criminological in nature. Given the nature of the area of study and the fact that it can be an illegal activity that is being committed during non-compliance, this makes sense.

Straub (1990) utilized the criminological theory of deterrence to determine the effectiveness of the IS security of an organization. Straub (1990) did find that deterrent administrative procedures resulted in lower computer abuse. Deterrents in the form of policy statements or, more specifically, a policy that requires employees to sign a data contract lowers computer abuse (Straub 1990).

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.

Though non-compliance is the end problem, a probable predecessor to non-compliance is resistance to the implementation of the IS Security policy. As discussed in chapter one, resistance to IS Security policy implementation is one of the major findings of the first case study that preceded this dissertation. After a review of the literature, it was determined that very little research had been undertaken in this area. As will be discussed below though, there have been some references to resistance in the literature.

Siponen (2000) took an organizational view to resistance by taking the perspective of a system's administrator when he wrote on security awareness. Siponen (2000) found that resistance may arise from a person seeing certain actions as totally wrong or deficient. Furthermore, he found that if guidelines (which typically take the form of policy) are so weighty and obligatory that they lead to prescriptive states, they can cause greater risks in the form of resistance. He found that some pragmatic approaches should greatly reduce such resistance. He prescribes that all actions should be logical. For example, it may not seem logical to a person not to be forced to change their password every week. If this is part of a new security policy, there is likely to be resistance. The next point provided is that actions should appeal to the emotions of those affected. Implementers should strive to make security measures that aim at provoking emotions and appealing to them in order to affect attitudes and motivation in a positive manner. The next point discusses ethicality and morality. If a security policy is founded on established moral and ethical principles, it is less likely to be resisted. Well-being and a feeling of security followed and allow for the user to act in self interest. For example, if it is well known that a security breach could bankrupt the company, it is in the employee's best interest to avoid this scenario by following the policy.

Outside of the realm of IS Security, there exist seminal articles in the IS literature that deal with resistance to implementation of IS. Both Orlikowski's (1993) paper and Markus' (1983) paper are well known and abundantly cited. Orlikowski (1993) found that resistance can arise from organizational change. Introducing a new security policy can be a form of organizational change. Specifically, she found that while the findings did not show that "structural, procedural, and cultural changes by business units will lead to the successful adoption of IS product reorientations, they do suggest that where such changes are absent, there will be significant problems of inertia, territorialism, and resistance" (Orlikowski 1993, pg. 37).

From a theoretical perspective, Markus (1983) identified three theories that might explain what causes resistance. These were people determined, system determined, and interaction theory. For people determined, the causes were internal to people and groups and included cognitive style, personality traits, and human nature. System determined referred to system factors such as ergonomics. These could include lack of user-friendliness, poor human factors, or inadequate technical design or implementation. Interaction theory dealt with the interaction between the system and the context of use of that system. Markus (1983) identified two major areas within interaction theory: sociotechnical and political.

Markus (1983) listed the typical organizational methods to reduce resistance. These were get top management support, provide technically sound systems, provide user friendly systems, and attempt to make the benefits outweigh the costs of the change. Her research found that the use of Interaction Theory proved useful in handling resistance. For one, if the implementer considers himself or herself as one of the parties in the analysis, they will have much more ability to understand other people's reactions to the systems the implementer is designing and installing (Markus 1983).

As was previously stated, there is very little in the way of specific research that deals with resistance to the implementation of IS Security policy. Markus' (1983) work dealt specifically with IS implementation and Siponen's (2000) work dealt with security awareness. There is a hole in the literature specific regarding resistance to the implementation of IS Security policy. What is needed is an approach to researching the phenomenon.

As a final note in the portion of the literature review that deals with IS Security policy, it is important to answer the obvious question: why might resistance to the implementation of IS Security policy be a problem? The argument is that resistance can lead to non-compliance which can then lead decreased potential effectiveness of the IS Security policy. The literature that discusses IS vulnerability follows.

IS vulnerability is best examined through the lens of risk analysis as system vulnerability is exactly what risk analysis is identifying. System risk has been defined as "the likelihood that the firm's information systems are insufficiently protected against certain kinds of damage or loss" (Straub and Welke 1998, pg. 441) To counter the potential loss, Straub and Welke (1998) propose that managers initiate a program that uses a security risk planning model, provides education in security awareness, and performs a countermeasure matrix analysis.

Vulnerability has been defined as “a weakness in the security system that might be exploited to cause loss of or harm to the asset(s)” (Gerber and Von Solm 2006, pg. 21). This weakness would likely manifest itself from non-compliance to IS Security policy implementation. Each policy item was formulated in response to identification of a particular weakness or threat. Whether it be sharing passwords, opening executable email attachments, or intentionally attacking an organization’s IS, non-compliance to IS Security policy implementation greatly increases the system risk of that particular IS.

### 3.4 IS Policy and IS Security Policy

The two major sections in this chapter covered the literature behind IS policy and the literature behind IS Security policy. It would be helpful to analyze the congruent and divergent themes present in each of the streams of literature. As discussed in the IS policy section, three major themes emerged from the analysis of the IS policy literature review: IS policy is an integral part of strategic IS strategy, the focus literature in IS strategy has focused on alignment, and that there is therefore an implication that alignment between IS policy and business policy is critical. Reich and Benbaset (2000) implicitly rejected this implication. In contrast to Reich and Benbaset (2000), Jarvenpaa and Tiller (1999) still made the logical conclusion that if IS policy is an integral part of IS strategy, and that business-IS alignment is a critical goal of IS Strategy, business-IS policy alignment would also be critical.

The themes that arose out of the IS Security policy literature were IS Security policy formulation, IS Security policy implementation (with concentrations in disaster, resistance, and vulnerability), techno-centric versus org-centric dichotomies, and government compliance. It seems as though the thematic areas of IS policy and IS Security policy more contrast each other than compare. The overwhelming focus in the IS policy literature has been on the IS policy being part of the greater IS strategy. The IS Security literature is more diverse and focused on the policy itself.

Why this is the case can be answered by analyzing the nature of the two areas. IS security is an abstract field that requires vetting and IS a tool that facilitates the communicative flow of an organization. The vetting required of IS security necessitates the existence and use of an IS Security policy. This explains the explicit focus on the policy itself in the IS Security policy literature. The IS policy literature however must make IS policy a part of the bigger picture of the organization. This is why partitioning IS policy as a part of the greater strategic plan and striving for the alignment of IS policy with the larger business policy has been the focus of IS policy literature.

The IS Security policy research stream though could be informed by the IS policy literature. Even though IS security and IS are two different animals, they are closely related. It might prove fruitful to the research community to explore IS Security policy explicitly as a part of IS Security strategy, as IS policy is a part of IS Strategy (Mintzberg et al. 2003). While some IS Security policy literature has implied that IS Security policy is a part of IS Security strategy, such as Trček (2003) who created a framework for IS Security management and policy formulation, there is nothing as explicit as in the IS policy literature.

Another informing area of the IS literature that could aid future research in the IS Security policy literature is the continuing call for alignment of business policy and IS policy. This could be reflected in the IS Security literature by an exploration of the alignment of IS Security policy with IS policy. It could also take the form of an investigation of the alignment of IS Security policy with IS policy (Doherty and Fulford 2006). A third potential area could look at how each of these three policy areas interact, contradict, and compliment each other.

### 3.5 Discussion

The purpose of this chapter was to thoroughly vet the literature that supports the research stream in IS Security policy. It was important to first review the IS policy literature before discussing the IS Security policy literature. This is because IS Security policy must reside either as a part of IS policy or alongside the IS policy.

This literature review found gaps in the literature but it also verified the need for research in the area of power relationships and resistance to IS Security policy implementation. As discussed in the second chapter, the first case demonstrated that the topic of power relationships and resistance to IS Security policy Implementation was identified as an extant problem. This complex construct of “power” must be vetted as thoroughly as security policy was in the previous sections. Thus two critical steps must be taken in analyzing the construct. First, an investigation of the various philosophical roots of power must be discussed. Second, an overview of how other IS researchers have used each of these philosophical roots of power in their research will give some foundation as to how to move forward with this research.

The discussion of philosophy of power will be grounded in the area of social theory and philosophy. Lee (2004) describes social theory as theory (as defined by Popper's four specific propositions for theory) about social phenomena (as defined by Schutz's distinction between first-level and second-level constructs). In the area of power, Clegg (2002) makes a connection between early social theorists and late twentieth century philosophers. Clegg (2002) describes a connecting line between Hobbes's seventeenth century work and Luke's more recent work. He does admit though that there is difficulty in fixing a coordinate on that line where recent debates might make an entry, such as those by Foucault and Giddens. Though there is a rich history on the philosophical roots of power, this discussion will focus on contemporary thinkers. Given the fact that they built on the ideas established by a long line of philosophers, modern theorists provide ample ground to stand.

One of the most widely cited social theorists in IS research is Giddens (Jones et al. 2004). Giddens is known for his work in developing Structuration Theory, which attempts to offer a middle way between two competing positions in social theory. On one hand, functionalism dictates that objective external social structures act on passive human agents. On the other, interpretive tradition sees society as an effect of human agency. In structuration theory, there is a view of social structure being produced by and acting back on the agents who are the subjects of that structure which they instantiate through their establishment of it (Jones et al. 2004). Notable studies that make use of structuration theory include those of Orlikowski (1993), (Nandhakumar and Jones 1993), (Barrett and Walsham 1995), and (Elkjaer et al. 1991). Though power is a part of structuration theory, it is not explicitly a theory about power. Clegg (2002) goes so far as to state that "structuration theory, once it is stripped down, offers the analysis of power little more than another, albeit complex, subjectivist position" (pg. 15).

Another widely known social theorist, particularly in the area of power, is Foucault. Unlike Giddens though, his work is not as influential in IS research (Willcocks 2004). Specifically, it is "surprising to find Foucauldian methods and concepts discussed so little, let alone digest and used, in the information systems field" (Willcocks 2004, pg. 266). Foucault is known for linking power inextricably with knowledge. His analysis states that power is situated among a cacophony of social practices and situations. The discourse within these social formations is manifested in an economy of discourse. For Foucault then, power is directly tied into the economy of discourse itself (Willcocks 2004). Foucault describes discourse as follows:

> "Discourses are not once and for all subservient to power or raised up against it, any more than silences are. We must make allowance for the concept's complex and unstable process whereby discourse can be both an instrument and an effect of power, but also a hindrance, a stumbling block, a point of resistance and a starting point for an opposing strategy. Discourse transmits and produces power; it reinforces it, but also undermines and exposes it, renders it fragile and makes it possible to thwart it" (Willcocks 2004).

Though not directly used in much empirical IS research, the concepts of Foucault can be seen in adjacent and supporting studies. Willcocks (2004) cites Introna's (1997) utilization of Foucault's power and knowledge duality used in conjunction with Clegg's circuits of power in order to explicate case studies of IS implementation. Willcocks (2004) also cites Brooke's (2002) call for the use of Foucault to move beyond the Habermasian framework employed by earlier IS work.

Lukes (1974) offers a theory of power that describes power as a result of three dimensions. This usurped previous work that had described power as having two faces. Clegg (2002) claims to be heavily influenced by the work of Lukes but disagrees on some key concepts. Dhillon (2004) points out that within the IS field the works of Keen (1981) and Markus (1983) seem to be influenced by Lukes. Dhillon (2004) goes on to point out that Silva and Backhouse (1997) use Clegg's philosophy when they argue that IS success cannot come about unless systems are institutionalized into organizations.

## 3.6 Conclusion

The goal of this chapter was to provide a thorough overview of the literature supporting IS Security policy. As IS Security policy is a subset of IS policy, the chapter began with a discussion of IS policy literature. Having a baseline understanding of IS policy assists in properly categorizing IS Security policy. While this is a practical objective, the review of IS policy also helped provide a comparable stream of IS research by which to reflect the IS Security policy literature. As was stated, this showed some interesting potential paths that the IS Security policy research stream could take.

Research that examined IS Security policy as an explicit part of strategic IS security planning could add to the literature. Furthermore, research that explored the alignment of IS Security policy to IS policy could constitute future research.

Besides these gaps in the literature, the literature review found that research in the area of power relationships and resistance to IS Security policy implementation was apparent. In the discussion section, an exploration of the philosophy of power, coupled with IS researchers use of power provided a view as to how the research in this dissertation could proceed. The following chapter will outline a theoretical foundation with which the research of power relationships and resistance to IS Security policy implementation will base its methodology. The philosophical perspectives of power shall be revisited with the intent of determining the best theoretical base for the conceptual framework. Once this has been constructed, the specific methodology will be outlined and substantiated. The substantiation shall consist of an analysis of the philosophical considerations of the researcher.

# CHAPTER 4 Theory and Methodology

## 4.1 Philosophical Foundations of the Research

The term “paradigm” has been used to refer to philosophical roots. This can be defined as “basic belief systems based on ontological, epistemological, and methodological assumptions” (Guba and Lincoln 1994, pg. 107). The four competing paradigms identified are positivism, postpositivism, critical theory, and constructivism. Despite the fact that Guba and Lincoln (1994) claim that any of these paradigms can be used in either quantitative or qualitative research, their implication that they are all used in quantitative research is unfair. It is widely accepted that the overwhelming paradigm in quantitative research is positivistic. This is not the case in qualitative research as positivistic and interpretive stand toe-to-toe in a confrontational manner.

The concept of philosophy is broken down to four concise concepts (Burrell and Morgan 1979; Denzin and Lincoln 1994; Lee 2004): ontology, epistemology, methodology and method. The first concept, ontology, has its origins in ancient philosophical traditions. The Oxford English Dictionary (OED) (2007) states that post-classical Latin ontologia is an alternative to metaphysica. This cites Aristotle's definition of the science at Metaphysics, where he describes it as the science or study of being, that which exists. From an Aristotelian perspective, Metaphysics would seek to answer the question of existence. It seeks to answer questions like what is reality, and what exists? What is the nature of those things? Do some things exist independently of our perception? What is the nature of space and time? What is the nature of thought and thinking? What is it to be a person?

From an IS researcher's perspective, one's ontology can be defined within a much more discrete lens than classic metaphysics. According to Lee (2004, pg. 5), "a scholarly school of thought's ontology comprises its members' foundational beliefs about the empirical or 'real' world they are researching." These foundational beliefs tend to fall along the spectrum of logical positivism and social constructivism. On the logical positivist end, the belief is that the physical and natural world is the only true reality. Social constructivists, on the other hand, believe that socially constructed realities (such as shared beliefs or culture) are realities unto themselves.

The second of the four concepts that make up philosophy, epistemology, is defined by the OED (2007) as the theory or science of the method or grounds of knowledge. Lee (2004) aptly points out that this definition is not very helpful because how can one study knowledge without utilizing knowledge, itself? Its circular reasoning seems to make it a non-entity. However, Lee (2004, pg. 6) goes on to conceptualize epistemology as "a broad and high-level outline of the reasoning process by which a school of thought performs its empirical and logical work." Therefore, the reasoning process by which an interpretivist (or constructivist) would investigate a phenomenon would be different from that of a positivist.

From an interpretivist perspective, this knowledge of reality applies equally to researchers and their subjects. This is described by Walsham (1993, pg. 5) by noting that "there is no objective reality which can be discovered by researchers and replicated by others, in contrast to the assumptions of positivist science." This perspective was echoed by Howcroft and Trauth (2005, pg. 33) who state that "interpretive researchers aim to develop idiographic theories pertaining to individuals in specific social settings and time periods." In other words, "Interpretive research provides in depth insights into social, cultural and historical contexts within which particular events and actions are described and interpreted as grounded in the authentic experiences of the people studied" (Howcroft and Trauth 2005, pg. 33). As stated in the first paragraph, this research is grounded in the interpretivist perspective.

The third and fourth concepts that make up philosophy are methodology and methods. Methodology refers to how the empirical or logical work is done. This is driven by one's epistemological and ontological perspective. For example, an interpretivist might employ grounded theory, ethnography, hermeneutics, action research, or case study. A logical positivist might use classic experimental techniques, statistical analysis, or case study. Note that in some instances, the same methodology could be used with different ontological perspectives. Regarding case studies, Myers (1994) has classified Yin as a positivist case study methodologist and Walsham as an interpretive case study methodologist. Within a methodology are methods that are used to conduct the empirical or logical work.

All of the above philosophical pillars of research are, "a basic set of beliefs that guides action" (Guba and Lincoln 1994, pg. 17) during the research process. The methodology will be discussed further in the Design section of the chapter. The methods will be discussed in the Data Collection and Data Analysis Techniques section.

## 4.2 Conceptual Framework

From Orlikowski (1993), to Giddens (1984), to Clegg (2002), there are a number of well thought out avenues by which to ground a conceptual framework of power. For this research, the most appropriate theory to ground such a conceptual framework is Clegg'g (2002) Circuits of Power. Clegg's (2002) claim that there is a direct relationship between power and resistance makes his theory, circuits of power, a solid fit to lay the groundwork for the conceptual framework. Furthermore, Clegg (2002) specifically states that "circuits of power" was built with the goal of being able to locate obedience and resistance.

The construction of a conceptual framework from this particular theory is not an easy task. The very word *circuit* implies a dynamic model that is never in the same state, temporally. This issue of a transformational model is exacerbated by the concept of episodic power that is a part of the model. Episodic power represents episodes of day to day interaction, work, and outcomes whether positive or negative (Clegg 2002). None the less, an analysis of a generic point in time in the model can provide the information necessary to create such a conceptual framework.

Clegg's (2002) circuits of power model (see figure 4.1) constitutes a discursive field of force socially constructed by human agency by virtue of organizing. Agency is defined as "something which is achieved by virtue of organization, whether of a human being's dispositional capacities or of a collective nature, in the sense usually reserved for the referent of 'organizations'" (2002, pg. 17). In the model, power moves in three dimensions, through three distinct and interacting circuits. Clegg (2002) seeks to open up the everyday machinery of power for inspection. This reveals that the process of organizing and involves techniques of discipline, which acts as causes of empowerment and disempowerment at the highest (macro) level of the model. The model contains three levels, two of them macro and one micro. Each of these levels will be discussed in the next three paragraphs.

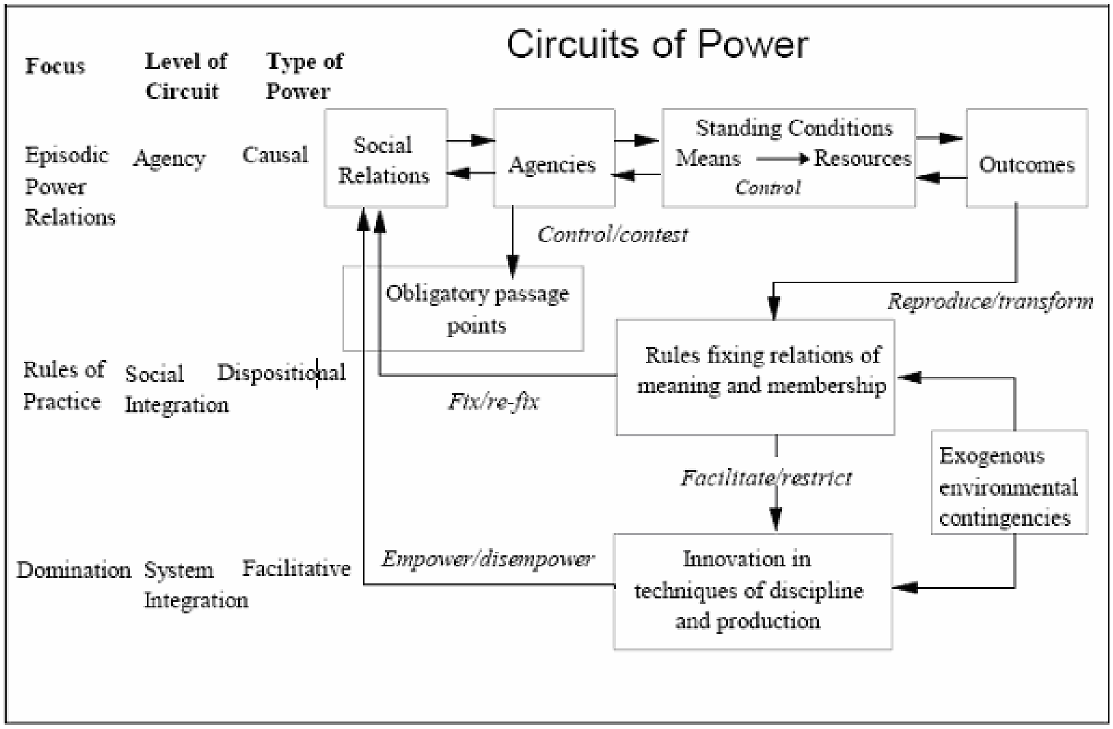


*Figure 4.1: Clegg's Circuits of Power*

The first level of the circuit is what is known as "episodic" (Clegg 2002). This refers to the day-do-day interaction, work, and outcomes. One-to-one communication and conflict and their consequences are part of this level. It essentially acts as a generator of data about power that informs the higher, macro, levels. At this level we see the "intermittent exercise of power" (Clegg 2002, pg. 187). Since "power always involves power over another, and thus at least two agencies, episodic power will usually call forth resistance because of the power/knowledge nature of agency" (Clegg 2002, pg. 208).

The middle level of the model (also a macro level), is the "dispositional" circuit, where rules socially construct meanings and membership relations. This circuit contains us/them dynamics, and mental maps or blueprints. Rules are fixed and re-fixed, and meanings are stabilized, through social integration (Clegg 2002). Authority is legitimated at this level. "Rules of practice are at the center of any stabilization or change of the circuitry. Through them, all traffic must pass" (Clegg 2002, pg. 215).

The highest macro level, the "facilitative" circuit, is comprised of systems of reward and punishment. Through the materiality of technology, job design, environmental contingencies, and networks, the facilitative circuit is "a major conduit of variation in the circuits of power" (Clegg 2002, pg. 233). Innovations in technology, and changes in disciplinary mechanisms in this facilitative circuit, will empower or disempower the capacity for agency in the episodic circuit. Recall that agency refers to a means to an end within an organization.

Tying the three levels together into a super circuit are the obligatory passage points. These are at the junctures where the three levels (or subcircuits) of power interact. The circuits are interdependent, and the obligatory passage points are the channels for empowerment and disempowerment. This refers back to the "information generator" analogy discussed in the preceding paragraph that described the episodic layer. However, control of extant obligatory passage points will serve to reproduce institutionally system-transforming change (Clegg 2002).

These identified components of Clegg's (2002) circuits of power Theory offer a solid foundation for studying resistance in organizations. A conceptual framework which takes these components and overlays the power issues as concerned with IS Security Policy is presented in table 4.1. The first column lists the four major components of the circuits of power and their respective subcomponents, as described in Clegg's (2002) model. The second column gives the major description of the component as cited by the seminal work, Clegg (2002). The final column gives the respective issues to study for the given power component. These issues are specific in nature and are intended to be utilized within an organizational setting.

| Power Element | Clegg's (2002) Description | Issues in regards to IS Security Formulation and Implementation |
|---|---|---|
| Episodic<br>• social relations<br>• agencies<br>• standing conditions<br>• outcomes | Episodes of day to day interaction, work, and outcomes whether positive or negative. | • What are the characteristics of the day to day social interactions between "managers" and "subordinates?"<br>• Does resistance impact the bottom line of getting things done at the organization?<br>• Is there an awareness of a sentiment of resistance in the organization?<br>• Has any direct impact come out of resistance in the organization?<br>• What are managerial reactions to subtle forms of resistance? |
| Dispositional<br>• rules fixing relations of meaning and membership | Socially constructed rules, membership categories (us/them), and mental maps or blueprints. | • Are there explicit power structures at the organization?<br>• Does the power behind explicit or implicit power structures get utilized when resistance arises? |
| Facilitative<br>• Innovation in techniques of discipline and production | Systems of rewards and punishment (disciplinary mechanisms) and the materiality of technology, job design, and networks. | • How is resistance dealt with at the organizational level when it becomes visible?<br>• Are there specific or sporadic consequences to resistance?<br>• If there are implied or specific consequences for resistance, are they enforced? |
| Meta-Circuit Influences<br>• Obligatory Passage Points<br>• exogenous environmental contingencies | Provides passage points empowerment and disempowerment. | • Are there any central points (human or procedural) that allow for members of an organization to circumvent power structures?<br>• If such points exist, how have members performed acts of resistance through such channels? |

**Table 4.1 - Conceptual Framework of Power**

## 4.3 Design

There are many different methodologies one could follow to conduct research including hermeneutics, action research, case study research and ethnography.  As previously stated, this research is conducted as an interpretive case study. Interpretive research does not predefine dependent and independent variables, but focuses on the full complexity of human sense making as the situation emerges (Kaplan and Maxwell 1994). Furthermore, Kaplan and Maxwell (1994) argue that the goal of understanding a phenomenon from the point of view of the participants and its particular social and institutional context is largely lost when textual data are quantified.

Klein and Myers (1999) propose seven principles for conducting interpretive field work. These are the fundamental principle of the hermeneutic circle, the principle of contextualization, the principle of interaction between researchers and subjects, the principle of abstraction and generalization, the principle of dialogical reasoning, the principle of multiple interpretations, and the principle of suspicion. The first principle, the hermeneutic circle, suggests that all human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form. This cyclical feedback loop is critical to the remaining six principles. Contextualization, for example requires critical reflection of the social and historical background of the research setting, so that the intended audience can see how the current situation under investigation emerged. Without having this context, understanding the whole would be impossible.

The second part of the term, “interpretive case study,” is case study. Outlining what a case study is will clarify why and how the methods are used. It is sometimes mistakenly believed that case study research cannot be positivistic in nature but it actually can. Orlikowski and Baroudi (1991) classified IS research as positivist if there was evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population. Yin (2003) reflects these values in his description of the five components of a case study design. These are a study's questions, its propositions, its unit(s) of analysis, the logic linking the data to the propositions, and the criteria for interpreting the findings.

On the other hand, interpretive case studies generally attempt to understand phenomena through the meanings that people assign to them. In contrast to Yin's implied deductive approach, other researchers note that "the interpretive analysis is an induction (guided and couched within a theoretical framework) from the concrete situation to the social totality beyond the individual case" (Walsham 1993, pg. 15). The relative realism described by Guba and Lincoln (1994) is captured when Walsham (1993) describes that there are no correct or incorrect theories but there are interesting and less interesting ways in which to view the world. Walsham (1993) describes a researchers use of a theory derives from his or her own personal experience and insight.

It is a common critique that case study research is not generalizable. Upon exposure to case study research, many immediately dismiss the findings as situation specific. Lee and Baskerville (2003) even point out that many qualitative (IS) researchers simply forgo claims to generalizability before the discussion begins. Given the fact that research that lacks generalizability also lacks usefulness (Lee and Baskerville 2003), case study research *in toto* may be perceived to be lacking in usefulness. This misconception is based on the fact that many researchers define generalizability solely as statistical generalizability. Essentially, statistical generalization is when a sample of data is generalized to a population (or universe). According to Campbell and Stanley (1966) statistical generalization asks the question to what population settings, treatment variables, and measurement variables can an effect be generalized? This is another way of saying that one can generalize from a sample to a population.

By its very nature, case study research cannot be statistically generalizable. It does not deal with large numbers of respondents to questionnaires with which the researcher can perform statistical analysis. Rather, the case study method "allows investigators to retain the holistic and meaningful characteristics of real life events – such as individual life cycles, organizational and managerial processes, neighborhood change, international relations, and the maturation of industries" (Yin 2003, pg. 2). So, the general assumption is that IS researchers have transferred, from statistical research to qualitative research, both the notion of sampling and the associated notion that a small sample size (e.g., only one organization) limits generalizability (Lee and Baskerville 2003).

On the surface, the lack of statistical generalizability would appear to be a failure on the part of case study research. In reality though, statistical generalization is not as relevant as it might seem for case study research. According to Yin (2003), cases are not sampling units and should not be chosen for this reason. If they are not sampling units, then they should not be analyzed or generalized in a statistical manner. Walsham (1993) tackles the issue of statistical generalizability from an epistemological perspective. This is that one's claim to knowledge (epistemology) and research methods are intertwined and affect one's ultimate goal in performing research. If one adopts a positivist stance, then statistical generalizability is the key goal. However, if an interpretive perspective is one's epistemological position, then the plausibility and cogency of the logical reasoning used in describing the results, along with the conclusions drawn from them are what the goal is (Walsham 1993). In other words, the validity and extrapolation from an individual case does not depend on the representativeness of such cases in a statistical sense (Walsham 1993).

Lee and Baskerville (2003) challenged the very foundation of statistical generalizability when they pointed out that it is actually a form of inductive logic. This refers to reasoning from data points in a sample to an estimate of a population characteristic. Or, more generally one has a set of particulars and from that set produces a general rule. To describe the problem of induction, Lee and Baskerville (2003) quote Wood as saying that in order to validate inductive logic, "we need an additional premise, such as [the] Uniformity of Nature assumption or: 'The future will be like the past'." Considering the difficulty in validating the Uniformity of Nature assumption, one can question the relevance of statistical generalizability. One would have to continually regress through the circular logic of the Uniformity of Nature in a vain attempt to validate inductive logic. This problem of induction is credited to an 18th century philosopher, Hume, and is sometimes called Hume's Truism.

When a critic points out the lack of statistical generalizability in case study research, the rebuttal can be a complex affair. The fact is that case study research has no need or desire to be statistically generalizable but that reply may seem like a cop out. Despite the fact that it may seem like a cop out, the lack of relevance for statistical generalizability as it relates to case study research is a true statement. This is the case, whether a person is coming from a positivist (Yin 2003) or interpretive (Walsham 1993) perspective. If one wanted to add to the discussion, they could include additional evidence to support their perspective. However, how one tempers their response can help the dialogue. Pointing out Hume's Truism (Lee and Baskerville 2003) may lead to conflict because it could be interpreted as calling a quantitative researcher's entire body of work into question. Perhaps, in addition to questioning the relevance of statistical generalization to case study research, a description of one of the two types of generalization discussed below would be the most powerful rebuttal.

Generalizing from description to theory is described by Yin (2003) as analytic generalization. This type of generalization means that previously developed theory is used as a template with which to compare the empirical results of the case study. He also calls this a level two inference. Quantitative research can also contribute to level two inferences but only after the statistical generalization (level one inference) is performed. Lee and Baskerville (2003) emphasize that it is important to not violate Hume's Truism when making this generalization to theory. Specifically speaking, "a theory generalized from the empirical descriptions in a particular case study has no generalizability beyond the given case" (Lee and Baskerville 2003, pg. 23).

Given Lee and Baskerville's (2003), and Yin's (2003) insights, case study research succeeds in this type of generalization, as can most other types of research. The level 2 inference of supporting or falsifying theories is a powerful facet of theory generalization for case study research. This type of generalization is what fuels the progress of social science as it has a direct impact on the theories that the science rests on.

A second type of generalization, generalizing from theory to description, is described as “generalizing from theoretical statements (in particular, a theory that has already been developed, tested, and confirmed, such as one reported in a published journal article) to empirical statements (here, descriptions of what the practitioner can expect to observe in his specific organization if he were to apply the theory)” (Lee and Baskerville 2003, pg. 23). Furthermore, “the generalizability of a theory to a description of the results that the practitioner would observe if he were to use the theory in a new setting – i.e., a setting other than the one(s) where the theory was empirically tested and confirmed – is arguably the most important form of generalizability in business-school research” (Lee and Baskerville 2003, pg. 24). This emphasis on practitioner orientation has been noted by other IS researchers whereby “the theories, ideas, models, issues for debate, and other constructs in this book were thus all, directly or indirectly, aimed to be of value to the practitioner” (Walsham 1993, pg. 253).

It is important to note that this particular brand of generalization resides along the same lines as research question of relevance. Gliner and Morgan (2000) call this the practical application of research. Guba and Lincoln (1994) describe a study’s relevance as its applicability or generalizability in their argument for qualitative research. Given the fact that case study research is contextually oriented, its generalizability in this fashion is far superior to that of traditional quantitative methods. This is because the outcomes do not have to be applied only in similarly truncated or contextually stripped situations as they do in quantitative research (Guba and Lincoln 1994).

Regarding the specifics of the proposed study, the intensive case study took place between February 2007 and July 2007 in the Richmond branch of a national financial organization. The specific data collection methods will be discussed in the following section. The entire staff of the IT department (with particular interest paid to the IS Security policy group) was interviewed. The IT department totals approximately 100 employees. Daily observations and intensive document review will accompany these interviews.

### 4.4 Data Collection Methods

The three major forms of data collection in this study are  interviews, review of documentary materials, and participant observation. This section is devoted to discussing the details of each of the three main forms of data collection. The most common method for qualitative data collection is the use of interviews and this method is discussed first.

Fontana and Frey (1994) identify three major categories of interviews: structured, group and unstructured. Structured interviewing refers to a situation where an interviewer asks each respondent a series of pre-established questions. Given the rigid and inflexible manner of structured interviewing, it is not appropriate for the interpretive perspective of this study. Unstructured interviewing, on the other hand, tends to be closely associated with participant observation (Fontana and Frey 1994) and breaks many of the "rules" of structured interviewing. These might include answering questions asked by the respondents and letting personal feelings influence the interviewer. Suspending these rules is a necessary component of ethnographic or participant observation research.

This research follows an interviewing style that falls between these two extremes: semi-structured interviewing. Using this technique allows for the interviews to be grounded in the conceptual framework (structured) but still allow for the in-depth necessity of interpretive research. Many IS researchers have utilized semi-structured interviewing techniques such as Earl (1993), Orlikowski (1993), Reich and Benbasat (2000), Willcocks and Kern (1998), Lin and Silva (2005), and Wilson and Howcroft (2002). To adhere to the interpretivist perspective, the interviews were not be taped. Instead, the researcher took notes during the interview process and performed a personal debriefing immediately after each interview. This allows for a thorough vetting and interpretation of the data.

The second major method of data collection was the review of pertinent documents. Given they are a critical element of the study, IS Security policy documents are the focus of this portion of data gathering. According to Hodder (1994), documents are close to speech and require contextualized interpretation. This follows along the lines of Klein and Myers's (1999) principles for interpretive research. Hodder (1994) treats written texts as special cases of artifacts that require similar interpretive procedures, meaning that the texts must be entered into a dialectic relationship between the cultural context and the context of the analyst.

The final method of data collection is observation. One advantage of the observational method is that it is unobtrusive and does not require direct interaction with participants (Adler and Adler 1994). The primary locale for data gathering via the observational technique is during meetings and informal gatherings. Policy group meetings occur regularly at the proposed site and taking observational notes of the interactions between policy makers provides insight into the power relationships among IS Security policy formulators. Doing the same at informal gatherings provides insight into the subjects of IS Security policy and an understanding of their reaction to the implementation of such policy.

### 4.6 Data Analysis

The data analysis consists of three linked subprocesses: data reduction, data display, and conclusion drawing (Huberman and Miles 1994). With data reduction, the potential universe of data is reduced in an anticipatory way based on the conceptual framework. Data display refers to the compressed assembly of data that permits conclusion drawing (see Appendix E for the analysis tables). These take the form of structured summaries, synopses, or networked diagrams linking the major topics revealed during data reduction. Conclusion drawing involves drawing meaning from the data where the researcher is the agent of interpretation. The tactics used for this final subprocess involves noting patterns or themes, clustering, comparison and contrast, and triangulation.

The majority of the process described above is simply a method for categorizing the data into manageable units. The substantive portion of the analysis process is the area where meaning is drawn from the data. As stated, the researcher is the agent of this interpretation but this agency must be couched within a defined and vetted theoretical framework (Walsham 2006). Otherwise, only subjective opinion would be the resultant output. As Clegg's Circuits of Power (2002) has formed the basis for this research, it also is utilized as the theory by which the data analysis was rooted.

As noted by Huberman and Miles (1994), a critical pretext to the data analysis is the proper management of the data. With 51 interviews, dozens of meeting observations, and 1000s of pages of IS Security policy on hand, proper data management is critical to successfully analyzing the data. A dedicated filing cabinet is reserved for the raw field notes, transcriptions, documents, and interpretive materials produced by the researcher. An indexing system is arranged that hierarchically classified the materials. At the top level, the data is separated by each of the four areas described above (raw field notes, transcriptions, documents, and interpretive materials produced by the researcher) as well as a planning area. Within each of these areas, the documents are indexed by date.

The raw field notes consist solely of the manual recordings of the interviews conducted at the organization (see Appendix D for the interview records). The documents consist of a combination of Security Policy documents and requirements documents. The interpretive materials consist of the partial analysis completed immediately after each interview (what was previously described as the "debriefing period"). The planning documents consist of interview templates, IRB approval documents, consent forms, and forms of non-disclosure. Upon completion of the research, the organization required that all policy documents be returned or destroyed so this portion of the data is no longer stored.

## 4.7 Evaluation

This research is evaluated based on Klein and Myers' (1999) set of principles for evaluating interpretive research. These principles include the hermeneutic circle, contextualization, interaction between subjects and researcher, abstraction and generalization, dialogical reasoning, multiple interpretations, and suspicion. The fundamental principle of the hermeneutic circle refers to the idea "that we come to understand a complex whole from preconceptions about the meanings of its parts and their interrelationships" (Klein and Myers 1999, pg. 71).

The principle of contextualization demonstrates the need for critical reflection on the social and historical background so that how the current situation emerged can be readily demonstrated. The principle of interaction between the researchers and the subjects shows the need for critical reflection on how the research data was socially constructed through the interaction between the subjects and the researcher. The principle of generalization refers to the relating of the "idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action" (Klein and Myers 1999, pg. 72).

The last three principles refer to requiring a degree of sensitivity on the part of the researcher to minute details of their data and findings. The principle of dialogical reasoning means that the researcher has to show sensitivity to vetting possible contradictions between the theoretical preconceptions and the actual findings. The principle of multiple interpretations refers to the researcher showing sensitivity to differences in interpretations among the participants to the same event. Finally, the principle of suspicion refers to the researcher being sensitive to possible biases and distortions by the participants.

### 4.8 Conclusion

This chapter outlines the theory, methodology, and philosophy of research that the researcher is guided by, doing his research. It also discussed the site of study and some of the preliminary findings at the site. One of the key discussion points was the interpretive nature of the proposed case study research. This is important because it clarifies the researcher's epistemological perspective and justified the methodology and methods proposed. Extensive discussion regarding the generalizability of case study research was provided in order to rebuff the anticipated critiques that will arise from the positivist majority of IS researchers.

# CHAPTER 5 The Case Study

## 5.1 Introduction

The argument presented in the introductory chapter states that by overlooking power relations, organizations would fall short of achieving the most effective formulation and implementation of IS Security policy. This argument is conducted through the analysis of power relationships in the headquarters of a large financial organization located in the central east coast of the United States, to be known as Millennium Bank.

This chapter is organized into five sections. The introduction describes the organizational hierarchy and security policy at the site in order to give a foundation and context for the research. The following two sections analyze the case through the lens of the distinct theoretical subconstructs: episodic power and social/systemic integration. The fourth section discusses the findings via responding to the emergent findings that were identified within the case analysis of sections two and three. After the discussion on various power relationships prevalent in the case study, the conclusions derived in the chapter are presented.

The research is conducted via interpretive case study at the aforementioned financial organization over the span of four months between March 12th 2007 and July 26th 2007. The interpretive analysis is "an induction (guided and couched within a theoretical framework) from the concrete situation to the social totality beyond the individual case" (Walsham 1993, pg. 15). Interpretive case studies generally attempt to understand phenomena through the meanings that people assign to the artifacts and processes studied within the scope of the research. The theoretical framework is derived from Clegg's (2002) Circuits of Power as described previously. The method involves data gathering primarily via semi-structured interviews guided by the theoretical framework.

The interviews focus on the upper level management of the organization, particularly in the Information Systems and IS security executive level management. Of the 44 personnel interviewed, 70% (31) of the subjects were classified as upper level management within the organization. These included the president (CEO), Chief Operating Officer, senior vice presidents (including the CIO, CISO and CFO), 11 division officers, and 11 managing officers. The subset of managing officers made up approximately 20% of the total managing officers in the organization. These specific eight were chosen to participate in the research as they were identified as key stakeholders in the IS security policy formulation and implementation process. Many of the upper level management subjects participated in multiple interviews. The remaining subjects occupied the operational level of the organization and included accountants, financial analysts, application programmers, and various security personnel.

This site was chosen because it happened to be the bank branch that housed the national level IT (NLIT) for the entire bank organization. Therefore, this site housed the group that was in the unique position of formulating the new IS Security policy for all of the branches of Millennium Bank across the United States. The new policy was the result of the movement towards governmental standards and guidelines for IT and IS Security. The movement towards governmental standards did not take into account the fact that organizations differ, and therefore their security requirements will differ (Baskerville 1993). This point brought up by Baskerville is relevant to this situation because each of the branches operated in a semi-independent nature. While national standardization for the entire organization is intuitively appealing, there may be unintended consequences due to oversight of branch-specific issues. Though NLIT was responsible for formulating the new IS Security Policy and were not directly a part of this branch, they did take advisory points from the IS Security executives.

As implied in the previous paragraph, there is a separate entity for national level IT (NLIT) for this organization. Most nationwide information technology activities are consolidated under NLIT. NLIT provides key technological support and other financial services product offices through its Service Delivery and Architecture and Standards divisions. The Service Delivery division is NLIT's operating arm, providing centralized computer and network services to the financial organization, including applications and the national communications network. The Architecture and Standards division develops long-term strategies for NLIT, and maintains the organization's information technology standards. Figure 5.1 below illustrates the meta-organizational structure of Millennium Bank (note that this is a slightly modified version of the actual organizational structure in order to preserve confidentiality):

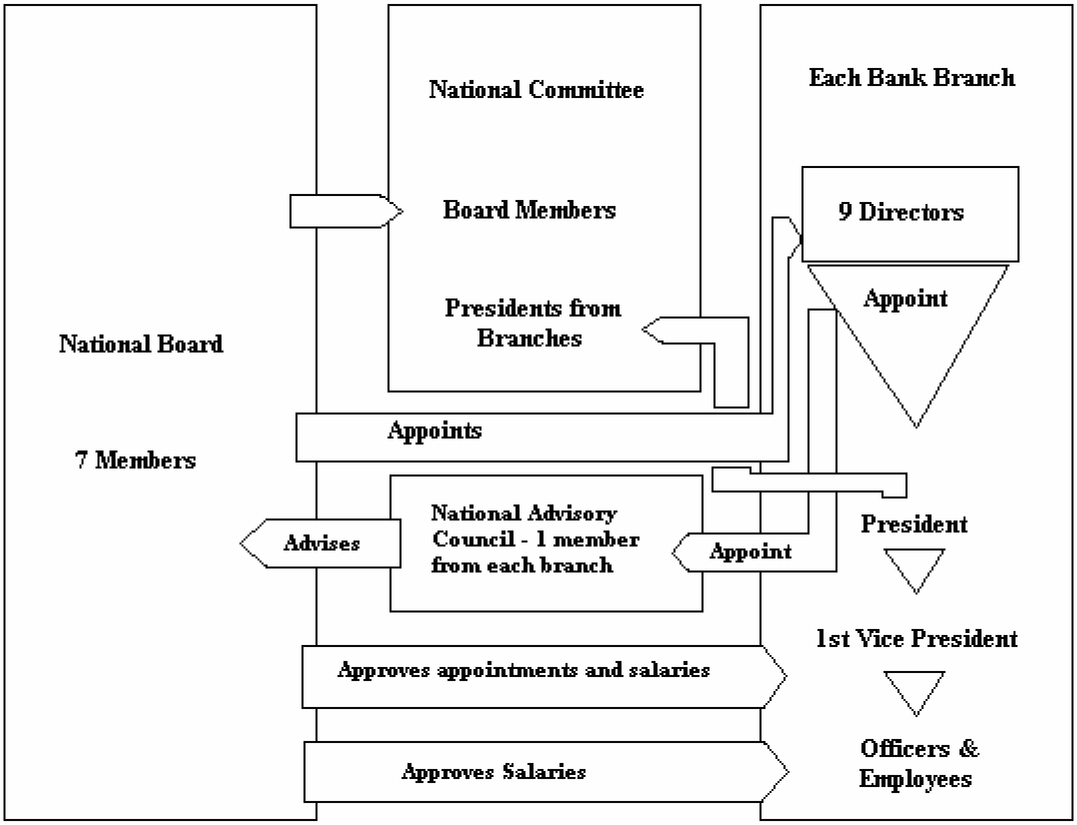


*Figure 5.1: Organization of Millennium Bank*

One of the responsibilities of NLIT is to formulate IS Security Policy. Within the NLIT, there is an IT Oversight Committee (ITOC). ITOC is responsible for setting strategic direction for the organization’s information technology, being the organization’s approval body for all national IT standards and security policies, and overseeing the provision of national IT services to the local offices and business functions. Though this external entity is responsible for formulating IS Security Policy, each branch of the organization is responsible for implementing the policy. There will be further discussion of this entity at both the resistance subsection of episodic power as well as the social integration section.

IS Security at Millennium Bank is designed to protect information from loss or misuse, and thereby to minimize the risk of monetary loss, productivity loss, or embarrassment to the bank. One component of the IS Security program is an information security policy that describes the procedures for maintaining confidentiality and integrity of information.

This policy requires each local branch with managerial responsibility for a business function to complete an information-security risk assessment to determine that the appropriate levels of security controls are in place. Risk assessments must address the risk of monetary loss, productivity loss, and embarrassment to Millennium Bank. The assessments consider both the likelihood and impact of the threats.

The applications, networks, and data centers that are critical to Millennium Bank rely on numerous security controls. These controls are routinely reviewed and enhanced. The security procedures include embedded protocols in the transmission hardware and software; identification codes, confidential passwords, and digital certificates used for access control; and traffic encryption across private or virtual private network connections. In addition, online participants must implement their own physical and logical security and management controls that appropriately protect the hardware, software, and access controls. Participants are also responsible for implementing any additional procedures set forth in the applicable security documentation provided by the local branch, as defined by the security policy. Offline security procedures include the use of individual identification codes provided by the local branch and may involve call back or listen back.

The first exposure employees have to the IS Security Policy occurs within the first few days of employment. All new employees are required to attend an IS Security training orientation process. The orientation involved sessions of videos, computer-based training sessions, and test taking. The videos were professionally shot and edited. The topics covered included excessive Internet use for personal reasons (including gaming, personal email, and day trading), swamping the network, password protection, and doing business for another entity. Failure to comply would result in an escalating series of repercussions including referral, remedial training, and for repeated offenses, termination. In addition to direct consequences, the video hints at the prospect of social shaming:

> "Besides being fired, you might find yourself mentioned in the local newspaper. Worse yet, there might be legal ramifications."

The computer-based training session covers important aspects of IS Security. It included information on how to create a strong password, how to spot social engineering scams, how to secure your workstation, and how to secure your work area. The training session is followed by an examination of the materials presented. Failure of this exam would result in remedial training and re-examination. This would continue until the employee was deemed acceptable by the security training manager.

This introductory section introducs the site by providing a discussion of the organizational hierarchy and the IS Security Policy at the organization. This context should provide the basis by which the case analysis can be framed. As stated, the analysis shall be discussed through the lens of the analytical framework provided in the methodology chapter. The following section begins this analysis through a discussion of the episodic power relationships at the bank.

### 5.2 Episodic Power

The circuit of episodic power (Clegg 2002) can illustrate the causal relationship between power structures and resistance. Episodic power refers to the day-to-day interaction, work, and outcomes. It is the most tangible of the circuits as it can be recognized by its outcomes, namely actions (Silva 1997). Silva (1997) goes on to note that the character of this circuit can be recognized by the relational nature of *A* having power over *B*. This "power over" relationship involves at least two agencies and will therefore "usually call forth resistance because of the power/knowledge nature of agency" (Clegg 2002, page 208).

This aspect of power is examined from specific perspectives from within an organization with regards to IS Security Policy formulation and implementation. First, the managerial relationships lay the groundwork for day-to-day interaction. Interpreting the reality of these relationships, in light of defined relationships as well as actual relationships, will help yield an understanding of how IS Security Policy is formulated and implemented. Secondly, the policy itself can act a tool of one or more agents in the power over relationship. As Clegg (2002) states, this type of relationship usually calls forth resistance. Thus, interpreting the nature of this resistance will broaden the understanding of how power relationships within an organization affect the formulation and implementation of IS Security Policy.

The analytical framework derived from the episodic circuit has identified two areas to study the way in which power relationships might affect IS Security Policy: managerial relationships and resistance to IS Security Policy implementation. The following two subsections discuss each of these areas and how the data is interpreted at Millennium Bank.

### 5.2.1 Managerial Relationships

The first area within episodic power is the day-to-day interaction, work, and outcomes. This is most often materialized within an organization as the managerial relationships. At the highest levels of the organization (executive officers, division officers, and managing officers), the relationships between subjects and their superiors is very casual and laid back. The upper level managers have considerable respect for their immediate supervisors (who included a handful of senior Vice Presidents as well as the President). This respect is bi-directional as they are typically allowed to "do their own thing" via a laissez faire management style. Also, the subjects are quite meta-cognizant of the underlying mechanisms that affected the relationship between themselves and their superiors. The Myers-Briggs personality index was mentioned by most of the executive level subjects. Since all of the subjects had taken this test and knew how each of their counterparts had performed, they feel they knew how to best deal with various supervisors and counterparts. Regarding conflicts at the highest level of management, the risk management officer said:

> "I interact with my supervisor daily. When we disagree, we always come to a reasonable conclusion. Since we're all working towards the same mission, we tend to be mutually encouraging to ensure accurate feedback."

This collegial atmosphere shifts more towards a stringent and project oriented perspective when subordinates are further away on the organizational chain. There is still a sentiment of mutual respect but "working problems out" was not quite as common as in the higher levels. For example, the business infrastructure manager stated:

> "When I interact with my subordinates, it's always project oriented. When conflicts occur, I'll listen to their input but almost all the time, they'll end up subjugating to me."

This high organizational level collegiality and organizationally distant but still professional dichotomy has been reported in the management literature (Smyth 1989). A unique aspect to this organization regarding management relationships is the semi-independent nature of all of the branches, including the research site. This meta-organizational setup has been evolving towards a more unified national arrangement since the September 11th, 2001 terrorist attacks in New York City. As this phenomenon had an impact on the rules governing the social integration and rules of practice, it will be discussed further in the dispositional power section of the case findings.

As stated, this management style is restricted to the upper tiers of the organization's hierarchy. At the lower levels, a higher degree of formality and process orientation is evident. Despite this reality, many of the managers noticed a relatively recent trend at the operational levels. This is that employees at the lowest levels of the organization have been more willing to disagree and speak up than they had in previous years. Despite increased likelihood of "speaking up" there has been a decreased level of explicit or implicit resistance to security directives.

Upon interviewing many of the non-management employees (including application programmers, accountants, finance, and network operations employees), an additional stimulus for this observation was discovered. There appeared to be a correlation between age/generation and willingness to confront or disregard authority figures within the organization. Those employees in the youngest age bracket (20-30 years old) were most likely to make statements such as this application programmer:

> "Half the time, the managers really don't have a clue as to what's going on. It's really easy to get around all the restrictions they put on us in the name of security. I get in arguments with my manager at least weekly but she never backs down."

Those employees in the older age brackets were more likely to just go along with the pack. Since this study is not longitudinal in nature, it is difficult to determine whether or not these employees would evolve into the more stable and less likely to confront older employee. This generational gap in attitudes towards work and management however has been noted in the literature. Specifically, those of the generations X and Y (born between 1960 and 2000) tend to reject the old chain-of-command system that goes with a traditional organizational hierarchy (Hersey et al. 2001). Furthermore, people of these generations tend to embrace involvement in decision making processes, skepticism, constructive feedback, and open dialog (Hersey et al. 2001).

While the generational issue is noted, it is not an overwhelming factor with regards to IS Security Policy acceptance. While younger subjects might be somewhat more likely to resist implementation of a security policy, older subjects are also found to question IS Security Policy implementation to a high degree. What this means in light of power relationships with IS Security Policy implementation is that resistance might arise. Hence, this particular topic area makes a logical transition to the next major subunit of episodic power: resistance. This major subunit will focus on resistance as it applies to IS Security policy implementation.

### 5.2.2 Resistance to the Implementation of IS Security Policy

Resistance is the second major subset of Clegg's (2002) episodic power circuit. During the course of the research at the site, the researcher moved between exploring perceived and actual resistance to IS Security policy. The distinction is made between perceived and actual resistance in order to obtain the most descriptive picture of the state of resistance at the organization. How resistance might be dealt with would differ if there is a disconnect between the sentiment of resistance and the actual state of affairs.

Regarding the subject's perception of the general attitude towards IS Security Policy implementation, there is a mixed response. Curiously, the highest levels of management mirror the non-management employees. This is to say that both groups always perceive a sentiment of resistance to new security measures. With that being said, the highest levels of management feel that the organizational collaboration is smooth enough to offset any negative outcomes. On the other hand, instead of the positive picture painted by the executives, the non-management employees have an air of bitterness. Their sentiments can be summed up by the following systems analyst:

> "Our jobs just got harder but what can we do? Our managers might listen to us but they won't change anything. With ISAF [a restriction of installing applications on office machines] in place, things are next to impossible to get done but we get by."

The group of subjects that made up the middle management did not see the sentiment of resistance that the higher and lower groups did. Most of them referred to the abundance of security awareness marketing that were such an integral part of life at Millennium Bank. To this group of subjects, it would be illogical that there could be an air of resistance when security is such an integral part of the culture of the bank. It is more likely that the motivation behind their answers arose out of self-protection. Since it is their job to ensure that their employees conform to the bank's policy, admitting that there is an air of resistance would imply they are not doing their jobs. The higher level executives however are more pragmatic in their perspective. Their responsibilities did not limit themselves to employees; rather the entire organization is their responsibility, thus giving them a greater level of clarity in their perspective.

Perception can be based of faulty and subjective conclusions, thus the research also includes a more concrete view of resistance. To understand this view, the researcher asked the subjects whether or not they had ever verbally or physically resisted IS Security Policy implementations. This question tended to come up in subsequent interviews, after the researcher had established a degree of trust with the subject, as it is a very sensitive and potentially incriminating question. The executive and middle level managers initially denied ever having done so but further probing revealed that they had indeed resisted at some point. The resistance took several forms including social engineering (Berg 1995; Jagatic et al. 2007), subversive resistance, and feigned ignorance (Scott 1985).

The most striking example of subversive resistance is described by the business continuity (BC) manager. The bank implemented a new security policy that required that all data tapes be encrypted. What this meant for the BC manager was that encryption machines costing in the hundreds of thousands of dollars would be required. He didn’t have a budget for these machines so decided to simply stop using tape backup. Even though the bank had used tapes for decades, this policy decision ended their use. He described the situation:

> “This ridiculous tape encryption policy caused me such a headache. I mean the tape backup center is five floors underground behind an armored locked door and is guarded by several armed guards. I could see encrypting the tapes if they had to leave the building but requiring every tape to be encrypted is ridiculous. They wouldn’t listen to me so I finally said forget it… we’ll just change over from tapes to disks to backup!”

This manager is at an executive level within the bank but his explicit position of power apparently did very little to get the policy changed. Through subversive resistance, he did find a way around the policy but the policy itself remained unchanged from its original form.

Regarding social engineering, this is referring to internal social engineering, and not external attacks. The infrastructure officer pointed out that the path of a given decision has a lot of variance. He said that, at times, he had invented a path just to streamline the decision making process. While he denied ever subverting security policy in any of these actions, his actions demonstrate a willingness to sidestep the organizational hierarchy via social engineering. The intentions were clearly not malicious and were in keeping with the bank’s mission though. The assistant VP of business continuity also discussed the way in which he had avoided bureaucracy by way of the trusted role. He pointed out that:

> "I have a circle of control and outside of that, a circle of influence. Even outside of the circle of influence, I am very trusted. If I ask for something, it'll get done. One's reputation could end up being a significant threat to an organization's IS Security."

He went on to say that it was unlikely that this threat would ever materialize because it takes years of trust building in order to be in such an influential position within the organization. The threat of social engineering is more geared towards fraudulent activity rather than insider threats (Ceraolo 1996).

The non-managerial employees acted out their resistance in a different manner than the higher level employees at the organization. Most of them stated that they openly resisted new measures verbally. For example, they would complain to their direct superiors. This perspective is verified by the middle and, to an extent, the upper level managers. An applications manager described his perspective:

> "Every time, my guys get hit with a new restriction, there's a lot of grumbling and complaining but nothing ever comes of it."

To further explore the issue of resistance towards IS Security Policy implementation, the research moved towards exploring the effect of the policy on work and productivity. While some employees may not intentionally resist security policy implementation, they might exhibit unintentional resistance if they felt their work and productivity were being affected. During the course of this part of data gathering, some contradictions in the responses were noted. Without exception, all of the employees (including middle and executive level managers) stated that their own productivity had been negatively affected by the implementation of various IS Security policies. They also agreed this had at one point or another resulted in intentional or unintentional resistance to such implementations. When the managers were asked whether or not any of their employees had ever experienced a fluctuation in productivity as a result of IS Security Policy implementation, the answers tended to be negative. The VP of Applications Development stated:

> "No, there definitely have not been any fluctuations in productivity. We are a very security-aware group. It used to be wide open though. Things have changed in the last five years."

The same subject had a different view of her own productivity earlier in the interview when she stated:

> "Yeah, some [security related] things have definitely slowed things down for me. They made a crazy password requirement for our Blackberries that put me out of commission for a week. More recently, they started a browser lockout that makes it impossible to do any web development."

This dichotomy demonstrates a logical fallacy that appears to be rampant throughout the various levels of management. The extensive focus on security seems to be blinding some of the managers to the reality of their subordinate's actions. It is also possible that this is simply representative of management saving face. The exceptions to this rule are the employees who were directly involved in IS Security Administration. They know that security was rarely a readily accepted reality in any organization and did not have many illusions about this fact. An executive level manager in the area of Infrastructure had previously held the position of Chief Security Officer (CSO) for the bank. He jokingly said that when he was the CSO,

> "If you were doing your job, I wasn't doing mine."

While the implementation of policy is clearly met with resistance and seems to affect employee's work and productivity, the question that remains is whether or not this resistance in turn affects the policy itself. There have been a few incidents at the bank where resistance has resulted in a change of security policy. The one most often discussed by the subjects (across the board of organizational levels and job types) is the blackberry issue. Blackberries are portable computing devices that allow for data to be stored and instant access to email. They are designed to be extremely portable, being about the size of one's palm.

Because of the sensitive data carried on these portable devices, the ITOC of the NLIT decided to formulate a security policy that required a very complex password that would protect the data in case the device was lost or stolen. A groundswell of opposition met the implementation of this policy. An executive level IT manager stated:

> "The Blackberry password requirement was absurd. It's not prudent to expect someone to remember a 15 character randomized string. I had to have mine reset half a dozen times after forgetting the password."

With the loudest voices being at the operational level of the organization, the NLIT, in conjunction with the branch's IS Security management, eventually decided to back down. As described in the literature (Mumby 2005), this is social control directed upwards. This and other observations at the organization support the contention that the traditionally disempowered employees can take control of the direction of the bank's security policy and forced a change.

## 5.3 Social and System Integration

The circuit of dispositional power is derived from debates about post-structuralism (Clegg 2002). The social integration level of the circuit's of power theory is concerned with "fixing or refixing relations of meaning and of membership" (Clegg 2002, page 224). It is also described as power that is embedded in the shared norms which bind the institution's cultural characteristics (Silva 1997).

In contrast to the day-to-day interactions described by causal power, dispositional power looks more at how social structures impact power relationships. With this perspective, the research now turns its focus towards two particular subunits within this level of Clegg's (2002) circuits of power: membership and shared norms. Membership refers to organizationally defined or implicit group structures within the organization. As an analogy, one could look at the example of a university organization that contains a promotion and tenure committee. This defined group might influence the power relationships within that particular organization. The second subunit, shared norms, can also be described as cultural characteristics (Silva 1997).

To better understand the context of the groups and membership within those groups, the culture and shared norms regarding IS Security shall first be described. Culture can be defined as "A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" (Schein 1992).

Within the confines of security, culture is defined as the totality of patterns of behavior in an organization that contributes to the protection of information (Dhillon 2007). In the previous section, a laissez faire management style was discussed. One might infer that such a style might also lead to a laissez faire IS Security Policy. In this organization this is a faulty and misleading inference though. This distinction is important to make because the literature has reported (Besnard and Arief 2004; Solms and Solms 2004) that a poor IS Security policy leads to a poor security culture.

Using Schein's (1992) three levels of organizational culture, one can quickly discount the inference that the laissez faire management style has resulted in a poor security culture. The first level, the security artifact, is abundant throughout the organization. Armed guards, locked and armored doorways, monitored hallways, and smartchip ID badges demonstrated physical security is critical. The second level, espoused security values, is evident throughout the organization. The site has banks of monitors in the hallways and lobbies dedicated to displaying various security propaganda such as "SEC_RITY is not complete without U!" and "Control + Alt + Delete When You Leave Your Seat." It is not possible to move around the organization without being subject to constant reminders of the importance of security. Also, as previously mentioned, every employee of the bank is required to participate in extensive IS Security training upon employment. The third level, underlying assumptions and values about security, came about during formal and informal discussions with many employees at the site. Not a single employee questioned the critical nature of security at the organization. An accountant described the embedded nature of IS Security at the bank:

> "We are hyper-aware of security here. I don't think I've gone a day in the last three years where someone hasn't mentioned something about security to me."

During the course of the research, three groups emerged as heavy influences on the way in which power relationships affect security culture at the bank. Two were formal membership groups and the other was an informal membership group. These groups were the executive level managers, operational level technologists, and the national level group (known as NLIT due to their responsibility for national IT) that was located at the branch. The executives and NLIT were considered formal membership groups and the operational level technologists were informal membership groups. The prior two groups had clearly delineated lines separating them from the rest of the organization while the latter group was not as clearly defined.

In identifying these social structures, the researcher probed the subjects regarding their perception of powerful groups within the organization. Despite the ambiguous classification, the most often repeated group mentioned was the technical subject matter experts, also known as technologists. The CSO said of one subset of these technologists:

> "The hardware guys can do what they want in terms of security procedures… I wouldn't know but fortunately, I do have a good relationship with them."

By "hardware guys," the CSO was referring to operational level employees in the IT support area of the organization. IT support employees are responsible for installing and maintaining all computer workstations, datacenter equipment (such as file servers, database servers and storage areas), network hardware (such as routers, switches, access points, and network interface cards), and portable devices (such as laptops, mobile phones, and Personal Digital Assistants [PDA]).

A second subset of technologists mentioned very frequently resided on the software side of the technological spectrum. These are the server administrators and are responsible for the setup and configuration of the centralized servers for the entire organization. The manager of Risk Management said of this group:

> "We depend on the server admins and are a little subservient to them. I'm not saying they run the show but do have a say in policy."

The Officer of Infrastructure agreed with this assessment adding the slogan, "Beware the power of the server admin." When interviewed, the server administrators had mixed reactions when asked about this sentiment. Like most of the operational employees interviewed, they felt organizational power was a function of explicit organizational hierarchy. For example, their boss held power over them and their bosses held power over them, and so on.

When pressed about how their technical knowledge and system access gave them an edge over people without such assets, the responses aligned with the personality type of the subject. There were 12 system administrators interviewed. Most (nine) of these subjects demonstrated characteristics that were consistent with an introverted personality type (Eysenck and Eysenck 1965). These included a lack of eye contact, limited discussion of the topics brought up in the questionnaire, and a lower tone. The introverted system administrators' thoughts on their potential for power are summed up with this young woman's comments:

> “Well… I don’t know what we’d do even if we knew something they didn’t. What motivation would I have to break guidelines?”

The three extroverted system administrators acknowledged having a close relationship with the IS security administration at the bank. They disagreed with the perception that their influence was a result of fear though. They felt that it was a mutual respect between their group and the upper level management of the IS security arm of the organization. They felt their insight actually helped with the formulation of effective IS security policy. Even though these employees are not part of the explicit (organizationally defined) power structure or part of the security administration they had influence on the formulation of IS Security Policy. One of them described the relationship as:

> “We all have the same mission in mind. The people over at NLIT will sometimes miss something important and I feel like we have an obligation to let them know. No one has ever questioned me going straight over there and letting them know about an issue.”

This phenomenon demonstrates that there is credence to the hypothesis that informal channels of organizational power might have an impact on the formulation of IS Security Policy. In this situation, the workers, or technologists, have an influence on the decision making process of the managers. This reality has been noted in prior research whereby workers were postulated to have agency despite the perception that managers always assumed to retain power over them (Orlikowski and Barley 2001).

Though identified as a power broker group, not all of the executives in the bank were responsible for implementation of IS Security Policy. This right exclusively lay with the IS Security executives. The head of this subgroup is the CSO. Though the CSO would "pull the trigger" with a particular IS Security Policy implementation, the decision would have to filter through to the myriad of middle level management before reaching the operational level. This caused problems with some at this first level of management. Many of them complained of a lack of clarity with the organizational structure. A database team manager said:

> "The structure is not well known or understood, especially taking the system and national perspective into account. I mostly don't know who decides what changes are made. It's like we're herding cats sometimes. It used to be clear cut but the scope of the security policy makes it less and less clear."

In terms of IS Security Policy formulation, the most critical of the three groups is the NLIT group. This is because this group did not directly answer to anyone at the organization (locally) but were responsible for the formulation of IS Security Policy. The introduction section of this chapter described the relationship between the local branch and the national level entity. To further the description, the functional subunits of the national level entity are actually split among the branches. This is not to say that they are subject to that particular branch's organizational hierarchy; rather they are simply geographically located at that branch. The NLIT functional subunit that deals with IS Security happened to be located in the same local branch that the research took place.

The interaction between NLIT and IS Security executives is restricted to the highest levels of the organization, specifically the CSO. Since NLIT's initiatives are intended to be national, all of the CSOs in every branch are involved in the advisory effort. To coordinate this, they created an advisory committee which meets regularly via teleconference. The intent of these meetings is to establish a consensus of advisory points for the NLIT towards formulating an IS Security Policy at a national level.

The researcher sat in on several of these tele-meetings. The dialogue at the meetings tended to be cordial and civil (mirroring the mutual respect of inter-executive dialogue at the local branch) but at times flared into disagreements. The content of the meetings is the minutia of details of merging the existing IS Security Policy with the emerging standardized policy. Some of the issues that came up appeared to be a conflict of competing status quos between branches. An example is illustrated in the following dialogue:

> Chair of Committee [remote]: "We don't need awareness in the end-user policy."
> Local CSO: "It's easier for me to enforce awareness if it is on the end-user policy."
> Chair: "We need to make it easier on the employee, not you."
> Local CSO: "That's fine and good but the typical employee doesn't…"
> Chair: [interrupting] "I think simple checkboxes done remotely would work fine."
> Local CSO: "We're talking a small amount of text here. It really isn't a big deal."
> Chair: [in an irritated tone] "Well let's just revisit this later."
> 3rd Remote CSO: "No, I think Frank [name changed] is right… let's just put it in the end-user policy."
> 4th Remote CSO: "Yeah, I want to be able to enforce this."
> Chair: "OK we'll put it in for now. I'd still like to bring this up at a later date."

As is illustrated, the 13 CSOs had preconceived notions and strong feelings about the content of the policy. They are passionate enough to demonstrate the weight of the advice they will be giving NLIT. Though they don't have the final say in the policy, their advice is likely to be the template for the final product. The three power broker groups all interact with the formulation and implementation of the IS Security Policy. This is to say that the technologists, NIST group, and IS security executives all impact the final outcome for the IS Security Policy.

With the impact of the organizational structures on the IS Security Policy understood it is important to also discuss the final circuit of the underlying theory to the analytical framework: system integration. In contrast to dispositional power, facilitative power is at the system integration level of the circuit's of power theory. It is concerned with the "empowerment and disempowerment of agencies' capacities, as these become more or less strategic as transformations occur which are incumbent upon changes in techniques of production and discipline" (Clegg 2002, page 224). Silva (1997) describes the main elements of system integration as techniques of discipline and production.

With Silva's descriptive thoughts in mind, when looking at IS Security policy formulation and implementation through the lens of system integration, the researcher is seeking understanding of informal compromises regarding resistance to security (production), procedures for dealing with resistance to security (production), consequences to resistance (discipline), and enforcement of those consequences (discipline).

From a production perspective, the data showed clear cut responses regarding how resistance to the implementation of IS Security Policy is handled. Generally, such resistance is ignored and referred to as grumbling and complaining. The resistance did not impact the formulation or implementation of IS Security Policy, typically. Some incidents did result in a change of formulation by vociferous resistance affected by the degree of impact on production and work. An example of this at Millennium Bank was seen earlier with the Blackberry password issue.

Regarding the second component of system integration, discipline, the data initially appeared to yield a consensus on how resistance is punished. The story told by executives, middle management, and operatives all described a procedure for dealing with resistance that included first having the employee's supervisor talk to them, followed by (for continued offences/resistance) remedial targeted security training, and finally termination. The executive level denied that it had ever gone as far as firing an employee.

Despite this apparent homogeneity on the surface, several middle level managers described cases where they had lost talented employees due to security violations. Many of the firings resulted from immediate action, without the trail of activities described by the majority of subjects. A financial team leader described such an event:

> "One of my best guys was canned last year for allegedly going to a pornographic site. The guy didn't get a warning or anything. One day, security showed up and removed him from the premises. I've been in contact with him since then and he has admitted to clicking on a link in an email but immediately shut down the browser when the site came up. I still can't believe nobody consulted me before the decision was made."

This scenario is not isolated to this particular organization. Substitute teacher Julie Amero faced up to 40 years in prison after being convicted of exposing seventh-grade students to pornographic images on their classroom computer in October 2004. She adamantly denied clicking on pornographic Web sites that appeared on her classroom's computer screen while she was teaching seventh-graders at Kelly Middle

School in Connecticut. Amero was convicted in January 2007 on four counts of risk of injury to a minor, but computer security experts and bloggers across the political spectrum rallied to Amero's defense when evidence later emerged that her computer had been infected with spyware that caused pop-up ads to take over the screen. On March 6, 2007, a $2,400 advertisement appeared in the Hartford Courant signed by 28 computer science professors who said that they think that Amero could not have controlled the pornographic pop-ups. On June 6, 2007, a New London superior court judge threw out the conviction of Amero. She was granted a new trial and entered a plea of not guilty. The new trial date has not yet been set; it is unclear at this time if the State's Attorney of Connecticut will pursue a second trial.

This issue is an ill defined area within security that could benefit from further research. It is not a question of workplace monitoring as it has long been established that organizations have the right to monitor employees. It is more a question of determining whether or not a serious breach such as this needs in depth examination to determine culpability or if immediate action (as described at the site) is appropriate. It is true that there are potential legal ramifications for an organization (Bequai 1998) but these extreme examples of miscommunication demonstrate that this issue needs further examination.

In contrast to this event, the Chief Security Officer stated that there is a fair amount of latitude in terms of dealing with resistance to security. Granted, the previous example is not necessarily indicative of resistance but it could be interpreted in such a way. From a security officer's perspective, if a policy has been implemented that forbids access to pornographic, gambling, or hate sites, not abiding to that policy (due to either intrinsic or extrinsic reasons) could be seen as resistance.

Despite the latitude described by the Chief Security Officer, many of the other subjects alluded to the strict enforcement of security at the bank. The perception by the operatives at the lower levels of the bank all referred to the senior leadership being very serious about security. A junior programmer stated:

"The bank has a very high ethics level. It's hard to sugar the facts."

The reality of the organization under study demonstrated the complexity of achieving an effective IS Security Policy. Though, on the surface, it appeared to be a bastion of a perfect instantiation of security, closer examination revealed cracks in the wall. From a deep culture of security to an active and determined security group, the organization is particularly intent on securing the organization. Their efforts appear to have paid off. However, there are social dynamics related to the implementation of security that continue to plague the bank despite the solid foundation.

## 5.4 Discussion

The mutually transformational relationship between IS Security Policy implementation, resistance, and productivity is an emergent theme that arose from this part of the research. It is found that there is a relationship between the implementation of IS Security Policy and resistance to the policy. The relationship manifested as direct correlation between the two events as an increase in resistance as a particular IS Security Policy item was implemented. This is evident in both the subject's perceptions as well as the subject's actions. The literature has suggested several causes to this perceived and realized resistance. Siponen (2001) reports that social implications of IS Security are at best afterthoughts. This is evident at the case under study given the informal and inconsistent way in which IS Security Policy is formulated. Furthermore, resistance can become an issue when users have no active role in IS Security development. The issue of lost work time and distraction due to the implementation of an IS Security Policy item can cause resistance as well (Besnard and Arief 2004).

Though not as strong a relationship as the effect of IS Security policy implementation on resistance, there still is evidence of the reverse end of that particular relationship. That is to say that the resistance has an effect on the implementation of IS Security Policy. It is plausible that a moderating factor to this relationship is the degree of impact the implementation of the policy has on productivity. Lost time from work and distraction is a potential cause of resistance (Besnard and Arief 2004; Schultz 2004). With this piece of the puzzle in place, the mutually transformational relationships can be seen in Figure 5.2:

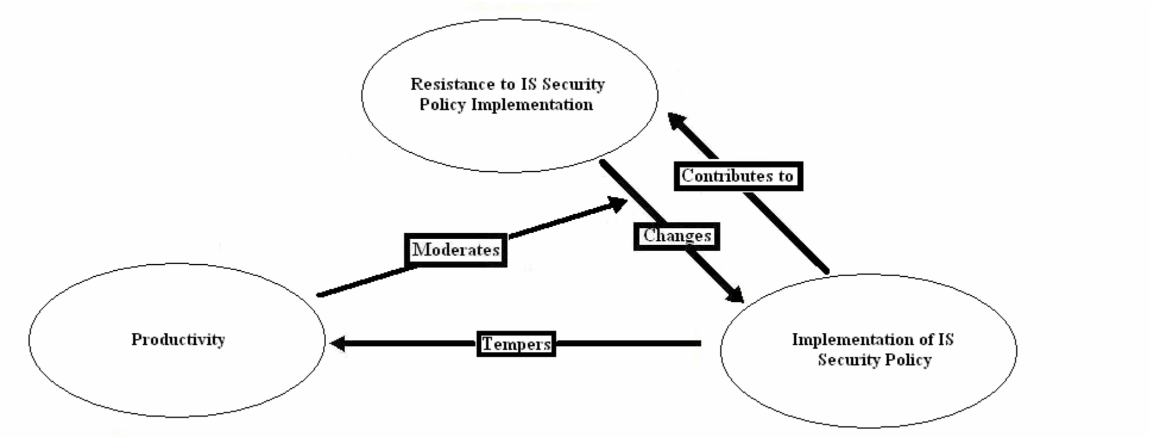

Resistance to IS Security Policy Implementation
Contributes to
Moderates
Changes
Productivity
Tempers
Implementation of IS Security Policy

*Figure 5.2: The relationship between IS security policy and resistance*

This diagram shows how there is a mutually transformative relationship between the implementation of IS Security and the resistance to that implementation. In other words, the implementation causes resistance to arise. This resistance may then change the implementation of the IS Security Policy. An important moderating element to this relationship is the impact that the implementation has on an employee's productivity in the workplace: the greater the negative impact on productivity, the greater the resultant resistance to the IS Security Policy. Negative impact on productivity refers to personal productivity. This means that though organizational productivity might not be affected by the implementation, personal productivity might slow down. Thus, the greater the resistance, the more likely it will cause a change to the policy.

This mutually transformative relationship will be discussed in considerably further detail in the upcoming synthesis chapter. Each of the relationships between the entities will be deconstructed and analyzed. Theoretical considerations such as institutionalization (Callon 1986) will also provide the basis for the analysis in the synthesis.

Regarding the formulation and implementation of IS security policy, the previous section indicated the influence of a particular subset of employees: the technologists. This observation is tied to a group of people with a particular knowledge base that have long been regarded as power brokers in organizations (Pettigrew 1972; White and Leifer 1986; Orlikowski 1993; Peppard 2007). The key differential point in this research is that it is not looking for the group's influence on the entire organization but rather specifically their influence on the formulation and implementation of IS Security Policy. The extent of this influence is dependent on the groups that formulate and implement the IS Security Policy. The group that is responsible for the implementation of IS Security Policy is at the executive level and are one of the three power broker groups discussed prior. The group that is responsible for the formulation of the IS Security Policy, the NLIT group, is the last of the three power broker groups.

The following scenario illustrates the influence of the technologists. A potentially problematic issue discussed with the CSO is that some policy items might not get implemented at the operational level due to the massive size and complexity of the IS security policy as a whole. When asked about this issue, the CSO acknowledged the potential for cracks to appear but felt confident in the fail stops. He went back to the technical group as his last resort. If IS Security Policy was not being followed, there was a good chance the technologists would catch it and notify the security group. For example, a strict password policy was implemented the year before the research began. Some employees continued to use simplistic passwords that violated policy. It would be very difficult for their managers or security staff to become aware of this lack of compliance because passwords, by their very nature, are confidential.

This is where the technologists would enter the picture. With permission from the security group, they would run cracking routines on the database that held the encrypted passwords. If any were cracked, the offending employee(s) would be notified and asked to create a stronger password. Most never had a problem and would comply with the request. Some however had to be disciplined. The security awareness manager described one employee in particular:

> “There was one who just refused to get the password straight. We warned him, had his manager write him up, and even sent him to remedial training. The fifth run through, he had actually hidden a message in his password that was clearly directed towards us [the security group]. It was an expletive and that was the last straw. He was terminated.”

As described above, non-compliance with very difficult to identify issues, such as encrypted passwords, are not above detection. The concern of middle management that the security policy implementation directives might get lost in the scope and complexity of the policy itself is likely caught at the technical level. This is a result of the IS Security Policy implementation being safeguarded by the technologists.

The interaction between NLIT and IS Security executives was restricted to the highest levels of the organization, specifically the CSO. Based on the preceding analysis, it can be seen that the three power broker groups described all have a specific influence on the organization’s IS Security Policy. The relationship between these power broker groups and IS security policy is displayed in figure 5.3:

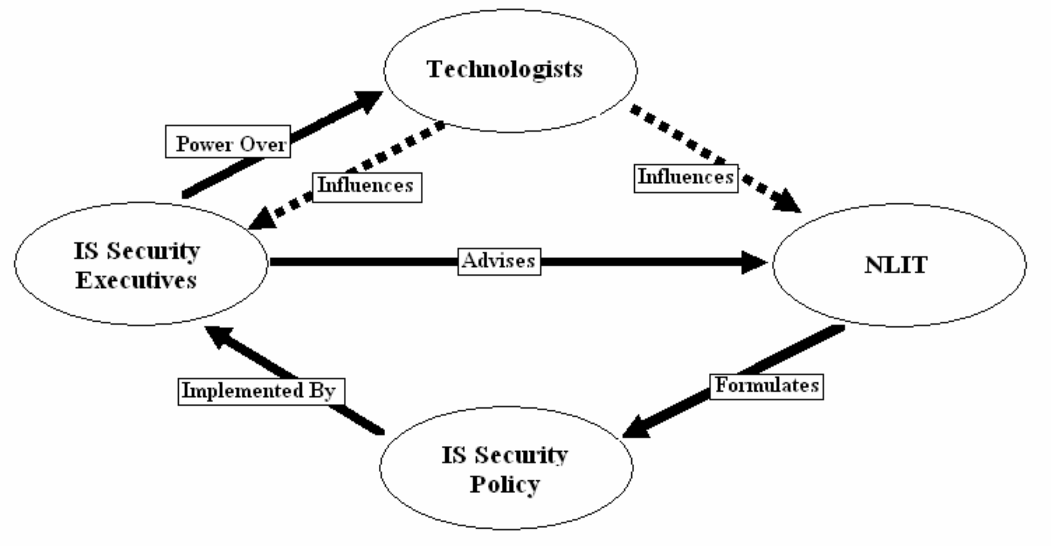


*Figure 5.3: The power brokers impact on IS security policy*

Figure 5.3 shows how the three identified groups that wield power within the organization in regards to IS Security Policy. That the national group formulates the IS Security Policy, the IS Security executives (CSOs) implement the policy, and the CSOs advise the national group is by design. That part of the relationship is not unexpected. The interesting aspect is the relationship the technical group has with the executive and national groups. This power relationship has a clear influence on both the formulation and implementation of the IS Security Policy. This phenomenon has not been reported in the security literature and is a fruitful area for future research. The extant literature that analyzes this phenomenon will be discussed in the following chapter.

## 5.5 Conclusion

In conclusion, there are several elements to the formulation and implementation of IS security policy that have not been operationalized at Millennium Bank due to a lack of understanding of the power relationships within the organization. Though the establishment has a well documented and planned set of processes in place for formulation and implementation of security policy, it fails to explicitly acknowledge the effect of resistance and implicit power brokers. The study of Millennium Bank's initiative to introduce a national level IS security policy reveals that a proper analysis of the power relationships could disclose some inherent complexity in the activities of the organization.

To carry out this analysis, on the one hand, an analytical tool is proposed: The Circuits of Power Framework, on the other, the nature of resistance and the effect of implicit power groups within the site is interpreted. As expected, there is clear evidence of resistance to the implementation of IS security policy within the organization. The nature of the resistance is heavily influenced by the perceived impact on productivity however. When the policy implementation effect on productivity increases in scope, the resistance to the implementation increases in voracity. It would appear that the entities responsible for policy formulation would be best suited in performing an extensive analysis on the impact a security policy might have productivity before implementation. Furthermore, a phased implementation would reveal unexpected effects before the organization were more profoundly impacted.

The second major finding of the case study is the effect of a particular implicit power group within the organization. This is the influence of the subject matter experts, or technologists, on both the formulation and implementation of IS security policy. The parties responsible for both formulation and implementation of IS security policy acknowledge, and to a degree expect, their input but it is at an informal level. It might be prudent to formalize the input of this critical group into the formulation and implementation processes.

This case study demonstrates that power relationships have a clear impact on the formulation and implementation of IS security policy. Though there is a strong security culture at the organization and a well defined set of processes, an improvement in the process and ensuing security culture is possible by accounting for the effect of power relationships.

# CHAPTER 6 Synthesis

## 6.1 Introduction

A synthesis, in philosophical systems influenced by Hegelian ideas, is the final stage of a triadic progression in which an idea is proposed, then negated, and finally transcended by a new idea that resolves the conflict between the first and its negation. In the philosophy of Kant, a synthesis is the action of the understanding in combining and unifying the isolated data of sensation into a cognizable whole. In a wider philosophical use, a synthesis is the putting together of parts or elements so as to make up a complex whole; the combination of immaterial or abstract things, or of elements into an ideal or abstract whole. In essence, this chapter will aim to answer the question begged by the research: *"so what does it all mean?"*

In this chapter, the aim is to provide an overall synthesis of the research findings and a discussion of implications for practice. This chapter provides an overview of the major research findings, a discussion of the significance, and a discussion of the major strengths and weaknesses of the work. The significance mentioned refers to the ways in which the research contributes to the field, that is, where it confirms previous work or breaks new ground, or the context in which the research should be placed, and the applications to practice the work suggests. This manifests the entire research agenda reflected in the dissertation, and synthesizes across the individual papers.

With this in mind, this chapter is organized into five distinct sections. After the introduction, the three research questions posed in the first chapter are revisited in light of the case study discussed in the fifth chapter. Though these questions where touched on during the course of the case discussion, a specific re-examination is prudent in order to provide a full disclosure of the findings. The third section specifically examines the major emergent findings of the study and discusses where they confirm previous work or break new ground. It also reveals the practical context by which the research should be placed. Finally the strengths and weaknesses of each major emergent finding are discussed.

The fourth section examines what the emergent findings might lead to in a philosophical sense. This is the final product of the synthesis in that it attempts to move beyond the literal findings of the research and into an abstraction of what the findings might mean from the structure of a philosophical framework. The final section, the conclusion, recaps all of the major points indicated during the discussion of the synthesis of the research.

### 6.2 A Re-Examination of the Research Questions

The argument presented in the first chapter states that organizational power impacts the development and implementation of IS Security policy. Furthermore, it is postulated that this relationship is bi-directional in nature; meaning that organizational power can affect how IS Security policy is conceived and implemented and IS Security policy can affect organizational relationships and interactions. This argument prompts three specific research questions: In what ways do power relationships within an organization have an impact on the formulation of IS Security policy? In what way do power relationships within an organization have an impact on the implementation of IS

Security policy? To what degree does the implementation of an IS Security policy have an impact on the existing power relationships within an organization?

The research questions are clearly analytical in nature and were designed in light of the methodology involved being an interpretive case study. On the spectrum of rhetoric of exploratory study described by Walsham (1995), the intent of this research is to reside within the stronger claims for the interpretive approach. The weaker end of the rhetoric often calls for interpretive research to later be subject to a more rigorous positivist approach. The implication of course being that interpretive research is not rigorous in and of itself. At a stronger level, researchers (Orlikowski and Baroudi 1991; Newman and Robey 1992) have called for the interpretive approach as a complement to positivist approaches. This research however bases in a stronger rhetorical level yet whereby it claims that the research issue at hand is best suited to an interpretive approach.

The justification for this claim is that positivist approaches are best suited to discover cause and effect relationships and power relationships are typically considerably more complex than such an approach would allow. It would be quite difficult to reduce the many constructs that might impact such relationships to simple variables. Understanding the context of such relationships is the ultimate goal and is in actuality the primary source of the research data. This approach is fundamentally interpretive. How each of the original research questions were revealed during the course of the research will be discussed in the following three subsections.

### 6.2.1 Power Relationships and Policy Formulation

The characteristics of the organization that lent to the context around the question "In what ways do power relationships within an organization have an impact on the formulation of IS Security policy?" are addressed in this section. A recurring theme found throughout all levels of the organization was the degree of collegiality present at close supervisory levels and the increasingly sterile social interaction at distant supervisory levels. An example of this phenomenon might include the manner in which senior management might interact with other senior management, middle management, and operational level employees. They are most likely to be amicable and casual with fellow senior management, less so with middle management, and completely process oriented with operational level employees. This phenomenon was not only mentioned by all levels of employees during the course of the interviews but was also observed by the researcher.

This is not a new finding as organization theorists have long noted this phenomenon as a natural result of group and social processes (Ostroff et al. 2003). In light of this research however, a contribution is noted from within the boundary of IS Security Policy. The dichotomy in communicative styles reinforces the existing and explicit power structures defined by the organization and it is stipulated that this would stifle those of lower power brackets to contribute the IS Security Policy formulation process. So, the first tangible observation in this organization indicated that the explicit power structures were designed to preclude the lowest end of the power spectrum, the end-users, from being involved in the IS Security Policy formulation process.

In IS Security literature, there appears to be some disagreement on the effectiveness of user involvement in the development of IS Security. In one case, involving users in the estimation process leads to irrational estimates of risk exposure (Baskerville 1993). Other work has found that explicitly involving the users in technically demanding security development has yielded a more successful implementation (Holmström 1999). Recent research has identified users' participation in the formulation process as a critical contextual factor in the successful application of IS Security Policies (Karyda et al. 2005). Traditional methods of security awareness and behavior modification have apparently had little effect on a typical user's security behavior and users themselves have called for a user involving approach (Albrechsten 2007). For the users, this would be a much more effective method for influencing user awareness and behavior.

This research is not necessarily calling for an increase in user involvement in the IS Security Policy formulation process. It is however noting that the existing power relationships are having an impact on the formulation process. Lamb and Kling (2003) have found that power imbalances frequently prevent users from making a real contribution to an Information System's development. If the managerial communication style took a more homogenous tone than the dichotomy that currently exists, the lower tier of the organization might be more inclined to contribute to the formulation process in an informal manner.

A second area identified during the course of the research by which power relationships had an effect on the formulation of IS Security Policy was the organizational shift towards national standardization. This movement essentially centralized the power structure responsible for formulating IS Security Policy. This approach has been reported as having a high potential for success when securing an organization's IT environment (Ferris 1994). Others have found this approach to have the potential for a less than desirable outcome because a policy must fit in with the organization's culture (Hone and Eloff 2002). Where each branch once was responsible for the formulation of security policy for that specific branch, there now exists a single entity that formulates the policy for the entire organization as a whole. While each branch still had input into the formulation process via advisory committees, the ultimate decision now rests in the national body. The contention presented is that the nationalization of the entire organization from disparate branches had an impact on the formulation of policy. Because it is deliberately designed in such a way, this is a logical observation.

This phenomenon however is the direct result of the efforts of standardization in an increasingly security-aware organization. According to the National Institute of Standards and Technology (NIST), the international standard for IS Security, ISO 27002 (emerged from ISO 17799) is a starting point for developing organization specific guidance. It states that not all of the guidance and controls it contains may be applicable and that additional controls not contained may be required. It is not intended to give definitive details. It is indeed this standard that is the basis by which the nationalization of the security policy formulation at Millennium Bank is based.

This standard began in the United Kingdom and was labeled British Standard (BS) 7799 in 1995. It was first published as an ISO standard in 2000 along with a second version of the original BS7799. The process by which this standard came into being was studied through the lens of circuits of power in 2006 (Backhouse et al. 2006). The study took the form of a case study and portrayed how the institutionalization of an *ad hoc* development process results from the interactions of power among the stakeholders involved. The results showed how the different interests and objectives of the stakeholders were influenced by exogenous contingencies and institutional forces.

A third area identified by the case study demonstrates how power relationships have an impact on the formulation of IS Security Policy by involvement of the informal of a set of traditionally disempowered employees. As previously described, these employees are those that are closest to the technological aspects of the Information System at the organization. They occupy the role of Systems Administrators and have wide recognition as the knowledge power brokers. Though they hold the lowest positions in the organizational hierarchy and are considered operational employees, very few question the degree of influence this group had on the organization. Many of the executive level managers even allude to a sense of fear regarding this group of employees. Though the group has no formal power relationship over other operational employees or management, they hold an informal power relationship in the way in which they are perceived.

This contradicts the first area observed at the site regarding the impact of power relationships on IS Security Policy formulation. That area implied that formal power relationships alone, as defined by the organization, dictated how the process of formulation proceeded.  This, on the other hand, implies that there exists a certain group of individuals who have an impact on policy formulation.  This group however is a special subset of employees who hold a special knowledge base.  They are the literal instantiation of the Foucaultian *power / knowledge* mantra.

In the IS literature, it is noted that this "inextricable intermingling of knowledge and power give rise to the construct of power/knowledge and highlights that before something can be controlled, managed, or governed, it must first be known" (Schultze and Leidner 2002, pg. 229).  This insight is exactly what the researcher observed at Millennium Bank.  This is to say that the "power over" that the managerial staff were designed to have over this group of employees was eclipsed by the fact that they did not understand the technological foundation which they were managing.  They simply had faith that those particular employees had the best interest of the organization in mind.

The research exposes three areas at the organization that indicate the way in which power relationships have an impact on the formulation of IS security policy. The first indicates that traditional hierarchical power structures reinforce the intentional design to restrict policy formulation along the lines of that hierarchy.  In other words, the nature of the discourse between executive managers and operational staff precluded staff involvement in the formulation process. The second area described the nationalization and standardization of the formulation process.  By centralizing the process, the organization effectively removed the power of policy discretion from the individual branch CSOs and gave it to a "national entity."  The third and final area revealed a notable exception to the observation of the first area. This exception involved the impact that a sub-group of employees had on the formulation process. This sub-group held an informal power status as a result of their retention of a special knowledge base that was beyond the scope of the managerial staff. This will be discussed further in the emergent findings section.

### 6.2.2 Power Relationships and Policy Implementation

The second research question moved from the policy formulation question and towards the way in which the policy was implanted. It involves examining the way in which power relationships within an organization have an impact on the implementation of IS Security policy. Several areas that spoke to this question arose during the course of the research. All of the areas are related to the overriding theme of resistance. The way in which certain groups resist policy implementation or perceived resistance spoke to the way in which power relationships have an impact on IS security policy implementation.

These areas were identified during the analysis of the data. Several logical inconsistencies in responses by managers are noted. Regarding the perception of resistance, managers stated that they had not noticed any sentiment of resistance by their coworkers. This was observed at every functional area of the organization except the security sub-department. Despite this strong statement by the management staff, virtually all of the operational staff claim that they always felt ready to resist new security implementations. They feel that most implementations of security policy would likely make their job harder and thus are ready to resist. This inconsistency is also noted when the subjects are asked about actualized resistance. Virtually all employees discuss how their productivity had been negatively impacted by various security implementations. The managers however claim that they have seen no fluctuations in productivity by their subordinates.

This phenomenon is particularly interesting because the operational staff were resisting in order to maintain existing power relationships in place. By working against the implementation of directives implemented by the security staff, day to day work would continue to be directed by their direct supervisors and not by new and emerging security directives. This oversight would continue unhindered by any potential new and emerging power relationships enacted by the security policy. It would seem to be in the manager's best interest to foster this resistance as it would more likely maintain their existing power relationships. It is likely that the action they took (consciously or unconsciously claiming ignorance to the sentiment of resistance) may actually foster the resistance in the end run. By denying the very existence of such a sentiment, they are relieving themselves of the responsibility of dealing with it.

This interpretation of events is reflected in Schultze and Leidner's (2002) study of knowledge management systems. They found that the organization they were studying was silent on issues of organizational power structures. Instead of seeing this as an instantiation of ignorance, they see it as a consequence of the commodification of knowledge and as a form of self-censorship contrived by the organization's own need to position itself within relations of power. Given their awareness of the institutionalization of security at the organization, the managers at the organization in this study were likely intentionally positioning themselves within the power structures.

In this area of the findings, there is a dynamic and multifaceted impact that power relationships have on the implementation of IS security policy. The first is that the operational staff, who make up the bulk of the organization, are ready to resist the implementation. Their statements all describe a frustration at their jobs becoming more difficult but another unknown facet may be their desire to maintain the status quo of the existing power relationships. After a time of becoming familiar with the nature of the organizational process and structure, a change is not likely to be welcomed. This is not a unique aspect to security implementation and has been noted over many years in general IS implementation (Zmud and Cox 1979; Markus 1983; Davis 1989; Joshi 1991; Orlikowski 1993; Cavaye and Christiansen 1996; Allen et al. 2002). The second is that the management denies the obvious existence of this resistance. It is postulated that this denial is a result of the managers desire to maintain the existing power relationships.

In light of IS security policy, this is a critical issue. The effect that power relationships are having on the implementation of the policy has the potential to have significant detrimental effects on the overall security of the organization. With power relationships undermining the organization’s fundamental push for more effective security, there is conflict. This conflict is inconspicuous enough to escape the notice of the employees responsible for implementation effort.

In this organization, power relationships have a complicated yet singular impact on the implementation of IS security policy. As the security policy implementation shifts decision making from the traditional power structure and towards security personnel, it inevitably leads to various forms of resistance. Even at an organization that is heavily oriented towards security, as Millennium Bank is, there is a perception that security initiatives make people's jobs harder.  This leads to a sense of resistance by the operational employees and this perspective is nurtured by the managers who stand to see their power base eroded.

### 6.2.3 Policy Implementation and Power Relationships

The final research question involves the inverse effect of the second research question: the impact that the implementation of the IS security policy has on power relationships.  Instead of seeing the resistance that came about as a result of the implementation, the research now focuses on how the power relationships themselves might have changed as a result of the implementation.  There are two major areas observed in the site that demonstrate to what degree the implementation of security policy has an impact on existing power relationships.  Neither of these areas strengthened existing power relationships; rather they demonstrate either a realignment of power between executives or an emergence of power by the operational employees.

The first area found executive level managers subject to various levels of loss of decision making powers. For example, a vice president was obligated to encrypt all of the backup tapes once the new tape encryption policy was implemented.  He not only felt it was unnecessary but ran into significant fiduciary issues with the implementation. In order to be compliant with the policy, he would have had to purchase several tape encryption machines at a cost of several hundred thousand dollars.  Though he was at the upper tier of the organization's hierarchy, he had no say in how he could do this part of his job. The implementation of the IS security policy had in effect stripped him of his discretionary ability that he had traditionally held in that part of the bank's operations.

A second, more fundamental example involved a manager who found one of his best employees suddenly terminated. The termination had come from the security area of the bank after they had determined that the employee had visited a pornographic web site on his bank computer. The manager did not question the legitimacy of the anti-pornographic policy but was outraged that he lost the employee without any consultation on his part. On a follow-up, it was determined that the web site visitation was likely unintentional (the audit log showed the employee had been redirected to the website from an internal email). Despite this, the termination was upheld. Given the fact that employee hiring, retention, and termination are traditionally decisions made by the manager of the hiring department, this event caused considerable consternation between some managers and the security department. In the end though, the decision made by the security department was upheld and the power relationship shift became institutionalized. Both of these examples are demonstrative of the realignment of power between non-security related executives and security management. The security management's discretion ultimately superceded the traditional areas of discretion held by non-security management.

The question that arises as a result of these observations revolves around security governance. This is because the way in which security is governed should tie in with the overall governance of an organization. Posthumus and Solms (2004)argue that "it is of vital importance that executive management teams, including boards and CEOs adopt a sound ISG framework” (pg. 646). This construct of governance integration might alleviate some of the issues observed at Millennium Bank due to problems with the perceived realignment of power structures. If all of the management of the bank saw security governance as part of the overall corporate governance, these social stressors might not cause as much angst.

A second example discussed earlier was the immediate termination of an employee, without the knowledge or approval of his manager, resulting from a policy violation. The chain of events that happen after a policy violation occurs is typically escalatory in nature, whereby an employee’s termination would occur after several attempts are made to ensure compliance. This is in line with the security planning models advocated by the literature (Straub and Welke 1998). In this instance, the employee had no warning and no course of action to argue his case. He was simply fired without notification. His manager went so far as to indicate that on one day, his employee was there, and the next simply gone. Even after the policy violation was found to likely be unintentional, the firing was not revoked.

The aftermath to such an action has the potential to be distressing to the organization including the potential for civil suit. Whether or not an employee pursues the legal option would likely be affected by the nature of the context surrounding the issue. It might be perceived as a deviant workplace behavior (Robinson and Bennett 1995) and thus raise the specter of embarrassment. Intentional or not, it also is a clear violation of IS security policy and would not be a sure case for the employee.

A second area observed during the course of the research was the temporary but significantly fundamental shift in power relationships that occurred during contentious policy implementations. The degree of contention with a particular policy was dependent on how much that particular policy was perceived as a threat to status quo. This status quo could be related to technological work load (web browser lockout), usage difficulty (Blackberry ™ password requirements), or organizational work load. When the change was dramatic enough, a tipping point was reached and the populous would rise up and challenge the implementation. This typically "power light" group surged and forced the executive level to change the policy.

This reactionary surge in resistance was described by Mumby (2005) as social control directed upwards. While the realization of such resistance was discursive in manner, its effect was tangible. It was observed and noted that much of the discourse came in the form of direct communication between the operational employees and the executive level, in essence cutting off the middle management. In most situations, the existing power relations were suspended for a time and the will of the operational employees superceded the decree of management.

During the course of the research, the bond between IS security policy implementation and power relationships is clearly strong. This is likely due to the very nature of the implementation itself. By having a policy override all other policies, the implementation is forcing a change in power relationships. Though very little resistance was noted at Millennium Bank with the inevitable power realignment between management, it did dampen the organizational climate. While management was aware of the need for security implementation, they were generally discontent. To a lesser extent, some situations of implementation yielded a temporary shift in power relations where the operational level forced a change in policy.

## 6.3 Discussion of the Emergent Findings

As discussed in the case chapter, two major emergent findings came about during the analysis of the data. The first involved the mutually transformative relationship between IS security policy and resistance. The second emergent finding described the specific way in which power relationships effected the formulation and implementation of IS security policy at the organization under study. This section will discuss the ways in which the research contributes to the field. The main element that makes up the analysis will answer the question, how does the finding confirm previous work or break new ground? Each of the two emergent findings will be discussed below, each in their own discrete subsection.

### 6.3.1 The mutually transformative relationship between IS security policy and resistance

The first emergent finding was illustrated in Figure 5.2 (pg. 107). Each of the relationships indicated in the figure shall be analyzed in light of the extant literature. A summary of this analysis can be seen in Figure 6.1 below:

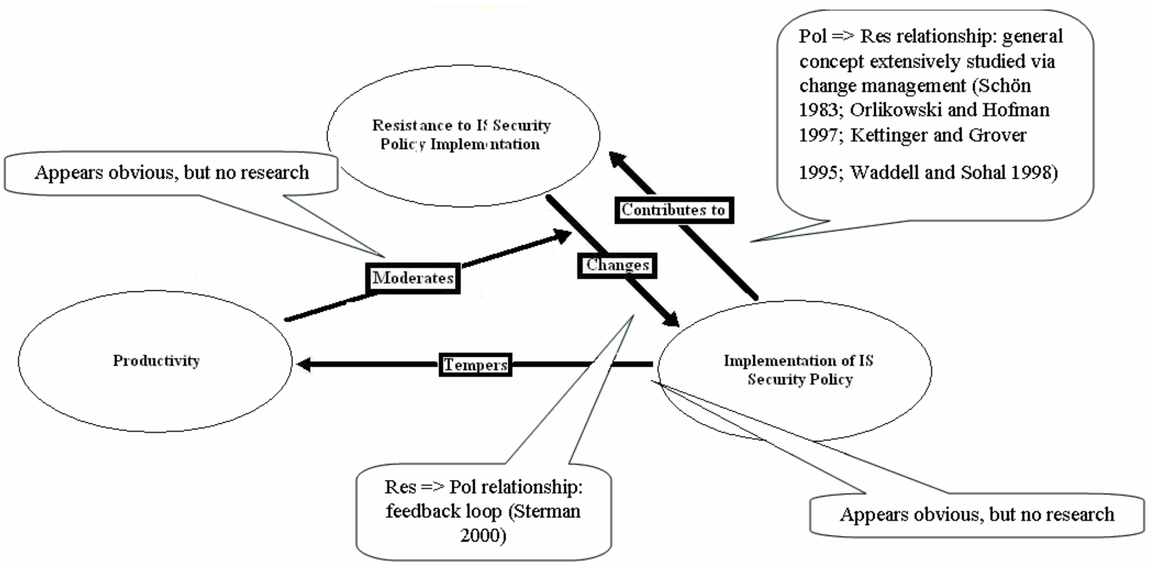

Pol => Res relationship: general concept extensively studied via change management (Schön 1983; Orlikowski and Hofman 1997; Kettinger and Grover 1995; Waddell and Sohal 1998)
Resistance to IS Security Policy Implementation
Appears obvious, but no research
Contributes to
Changes
Moderates
Productivity
Tempers
Implementation of IS Security Policy
Res => Pol relationship: feedback loop (Sterman 2000)
Appears obvious, but no research

*Figure 6.1: Analysis of the Relationships in the Policy Resistance Model*

The totality of the overall model is a unique contribution made by this research, but each relationship, by itself has had some discussion. The model details the interaction between the following four conceptual relationships: The implementation of IS security policy results in resistance (Pol => Res); Resistance to the implementation of IS security policy results in a change to that policy (Res => Pol); The implementation of IS security policy causes a negative impact on productivity (Pol => !Prod); The greater the amount of negative impact on productivity causes an increase in resistance to IS security policy implementation (!Prod => Res).

The first of these relationships, Pol => Res, was verified by virtually every subject at the organization. Some may interpret this as a simple instantiation of change management. Management and Psychology literature have indicated several methods for dealing with resistance including the Formula for Change (Beckhard 1969), alternate reinforcement (Niven 1990), attitude accessibility (Fazio and Williams 1986) behavior modification (Skinner 1938), change management (Schön 1983; Kettinger and Grover 1995; Orlikowski and Hofman 1997; Waddell and Sohal 1998) and system dynamics modeling (Sterman 2000). Some might argue that this is an area that has been thoroughly investigated. However, this research contends that the implementation of security policy is tied closer to the issues revolving around power relationships rather than managerial or psychological concerns.

Considering the fact that it is the management themselves that are subject to the realignment of power structures, it would be a conflict of interest to try to find a managerial solution to the issue at hand. A more appropriate approach would be to identify how to mitigate the perception of a loss of power due to the implementation of such policy. Strategically speaking, Mintzberg (1992) advocates clarifying organizational context and studying why some organizations thrive for many years. Another approach to strategy already discussed involves integrating the governance of security with overall corporate governance (Posthumus and Solms 2004).

An abstraction of the second relationship, Res => Pol, has been analyzed in systems research. Sterman (2000) describes a feedback loop (Figure 6.2) by which the actions of others affect the environment of the organization. This then affects the underlying goals which then finally impact the decisions behind the policy itself. This feedback loop also indicates the fourth relationship, !Prod => Res, if one views productivity as an aspect of the organizational environment. The model is presented as a method to discover and represent the feedback processes, which along with stock and flow structures, time delays, and nonlinearities, determine the dynamics of a system. In this way system dynamics might help avoid policy resistance. While this may seem to speak to the first relationship of the mutually transformative relationship of resistance and IS security policy implementation, it also refers to the effect of policy on the implementation. An analogous theory is presented by Mattia and Dhillon (2003) in the form of double loop learning for IS security frameworks. Figure 6.2 illustrates the feedback loop:

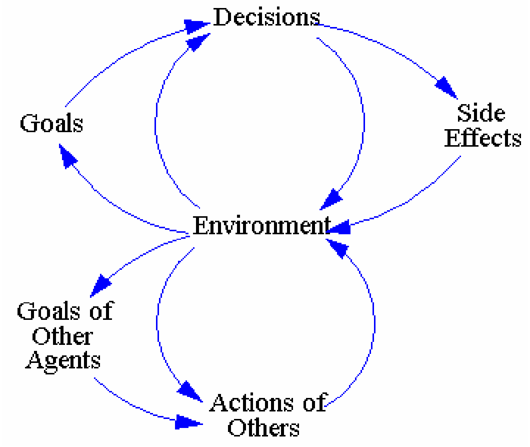


*Figure 6.2: Dynamic System Feedback Model*

What differentiates this research from the work done in systems research is that this research contends the primary cause of resistance is the inevitable effect policy implementation has on power relationships. While the systems feedback model offers a generic analysis in that the implementation might have some side effects and environmental impact, this research goes specifically to the root of the problem: power relationships. Instead of interpreting policy as a simple decision tool, it is presented that

IS security policy implementation must be a power redistribution tool. In line with overall corporate decision making, generic policy implementation would fit Sterman's (2000) feedback model. Policy implementation through the lens of IS security however, takes a new light. It impacts those that traditionally make the overall corporate decision and thus realigns the power structure.

It is this dichotomy that allows for the relationship to exist. At Millennium Bank, the operational staff would not be likely to resist an organization-wide policy implementation that required employees to wear business formal attire every day. It would be seen as a management decision. If however a security policy implementation came online that was perceived to come from a subset of management (security management), the door to resistance might be open. Considering security is not indicative of the entire management personnel, overturning an unpopular policy implementation might be perceived as more likely.

The third relationship, Pol => !Prod, is a domain restricted to the IS security realm given the nature of security being perceived as a "necessary evil." General business policies typically are designed to enhance productivity. The immediate affect of productivity loss may overshadow the long term potential gain of productivity by avoiding the information asset loss. This particular relationship provides an unexpected discussion point. Despite the widespread acknowledgement of this relationship from the subjects at the site, there is virtually no research that analyzes the phenomenon. The existing IS security literature that discusses IS security policy generally falls along the lines of models for formulation (Ferris 1994; Anderson 1996; Gritzalis 1997; Ward and

Smith 2001; Baskerville and Siponen 2002; Rees et al. 2003) and implementation strategies (Kühnhauser 1999; David 2002; Solms and Solms 2004; Doherty and Fulford 2005; Doherty and Fulford 2006).

There is a significant potential for future research regarding this relationship. The lingering question regarding the extent to which policy implementation actually (versus the perception of a negative impact on productivity) impacts productivity could be addressed. Furthermore, determining how an organization might mitigate both the perception and actualization of productivity loss when an IS security policy is implemented could be analyzed. The model as a whole also provides grounds for future research. Understanding the totality of the relationship could give practitioners a methodology to lessen the impact or correct misperceptions.

### 6.3.2 The power brokers impact on IS security policy

The second emergent finding, illustrated in Figure 5.3 (pg. 110), is also a unique contribution made by the research. Unlike the previous subsection, which focused on each relationship of the model, this subsection will discuss the primary aspect of the unique contribution: the effect of operational level, technically knowledgeable individuals on the formulation and implementation of IS security policy. The justification for this is that the relationships describing the entities responsible for the formulation and implementation of IS security policy are unique to this organization and may not be representative of other organizations.

Though this may be considered partially an organizational issue and not an Information Systems issue, the greater the interaction between the fields of information technology and organization studies should be viewed as more than a matter of enrichment (Orlikowski and Barley 2001). Information Systems literature has frequently examined the interaction between technologists and the overall firm. Jarvenpeena (1991) studied executive level involvement in the management of technology. While claiming even then that this area of study was well traveled, it was still determined that the actual level of involvement was stymied due to lack of an appropriate knowledge base by the executive level. While the task was commonly delegated to IT professionals, it was determined that it was "too important to leave to the hands of technicians" (page 205). The implication being that the power relationships focused too heavily on the technologists instead of management.

Tan and Hunter (2002) call for an understanding of the cognition of users and IS professionals. Regarding executive level management, this perspective could provide interesting avenues of future research. As newer generations of individuals with a more technocentric background begin to fill executive roles within organizations, it is likely that this technical gap between management and technologists will shrink. This would have a clear impact on power relationships within organizations as the reliance on technologists would be less profound. This source of power is known as "resource dependence" (Markus and Bjorn-Anderson 1987).

Another approach to reducing the impact of resource dependence was proposed whereby more frequent communication and the use of richer communication channels would result in a convergence of understanding between providers and users of technology (Lind and Zmud 1991). While this approach is designed for IT innovativeness, it could easily be applied to IS security policy formulation and implementation. Management at Millennium Bank was concerned about the potential for abuse by the systems administrators. They felt their only choice was to trust them and hope that they were doing the right thing. If management spent more time trying to understand the boundary and scope of the technical aspects of the system, they would be less reliant on the technologist's skill set.

A final perspective on the nature of resource dependence of executive management and technologists calls for a significant shift in the balance of technological power from the technologists to management (Nelson and Nelson 2003). This perspective is advocated based on the idea that organizational strategy should be driven by management and not technologists. Management personnel are deemed to have the foresight and awareness to guide the organization to a successful outcome. In light of IS security policy, this may be an unreasonable stance. Employees generally enter a firm with a finely honed skill set, whether it is financial, technical, logistical, or managerial. In order for a power shift to occur from technologists to management, one would expect management to absorb the skill set that the technologists brought to the firm. This would likely take away from the managerial skill set that their job calls for in most cases. As the power relationships observed in Millennium Bank are built on an existing knowledge base, this is essentially an impossible ideal.

This emergent finding has considerable potential for examination in future research. While the relationship between technologists and management has been studied extensively in general IS research, there is very little in the way of IS Security research that explores this phenomenon. Some questions that could be answered include: In what ways do technologists communicate there IS security policy suggestions in light of their position of power? In situations where technologists are left out of the loop, is the security of the firm left in a less effective state than where technologists are openly welcomed by the management staff?

### 6.4 Implications of the Findings

The chapter has addressed both the literal findings as related to the original research questions as well as the emergent findings. The question that remains is what these findings might lead to. The theoretical framework that guided the research, circuits of power, has been described as a framework for studying institutionalization as an outcome of power (Silva and Backhouse 2003). Given this, the natural implication arrived after the analysis of the findings is that the study revealed that the political processes involved in the formulation and implementation of IS security policy are both a result of and an agent towards the institutionalization of IS security at the organization.

Institutionalization has been defined as "an outcome of on-going struggle between different groups who have unequal access to valued material and symbolic resources rather than the result of an unmediated meeting of minds" (Foucault 1977, pg. 149). This dismal view of institutionalization perceives a negative connotation of the process, meaning it is forced on an organization by struggle instead of discourse. Lamb and Kling (2003) describe institutionalization as "the process by which an organization develops a distinctive character structure — a set of norms and routines, a way of doing things" (pg.

202). These processes are dialogical in nature and can take the form of normative, cognitive, or regulative interactions that produce a routine character structure.

In light of the theory guiding this research, these interactions can be defined along the lines of episodic power. Silva and Backhouse (1997) argue that the process of deciding whether an information system is institutionalized or not can be understood better by examining its political dimension. As Lamb and Kling (2003)operationalized institutionalization, Silva and Backhouse (2003) state that the institutionalization of an IS is operationalized when the stabilization of its processes have reached a point where its associated practices become routine. While Silva and Backhouse's research focused on general IS implementation, this research looked at the formulation and implementation of IS security policy. This distinction, though notable, is overshadowed by the parallels in theory. With this said, the significant question remains: To what degree is IS security policy institutionalized in Millennium Bank?

Silva and Backhouse (2003) describe how Circuits of Power relate to institutionalization as follows: Through dispositional and facilitative power, A makes B use a system. After repetition and routinization, the system is institutionalized. In the case of Millennium Bank, the first part of this equation is relatively clear when an IS security policy is implemented. The "A" actor is the security management and the "B" actor is every person in the organization. What makes this case interesting is that the site had only begun to implement the policy. The data was gathered at a time when the organization was experiencing an upheaval in the status quo of security.

At Millennium Bank, the institutionalized, “routinized” IS security policy had been in place and mostly static for almost 20 years. It was the required shift towards a national standard that brought about the new policy. The short answer to the question at hand is that the emerging IS security policy was not institutionalized at Millennium Bank at the time the researcher was collecting the data. The final step in Silva and Backhouses’s institutionalization model, repetition and routinization, had not come to fruition yet. Given the state of affairs at Millennium Bank though, an addition to their model became apparent. A recurring theme noted during the course of the research was the immediate resistance that most IS security policy implementation met. At times, this resistance would actually yield a change in the policy. This phenomenon is illustrated in Figure 6.3:

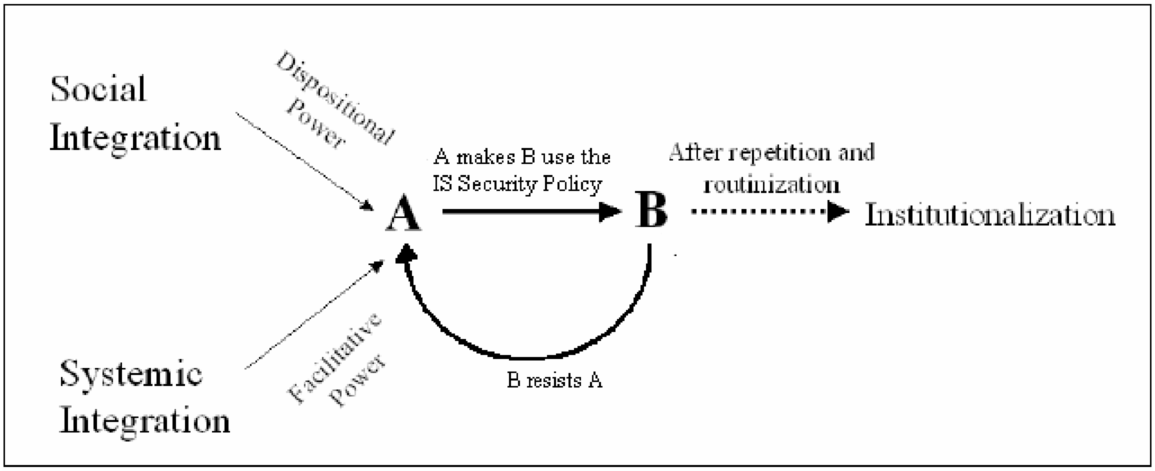


*Figure 6.3: Modified Model of Institutionalization*

Note the feedback loop from B to A. This modification to Silva and Backhouse's model is necessary given the data gathered at this organization. There were clear instances of resistance in certain situations where B was made to use the system (i.e. policy) mandated by A. Sometimes A would push back and force B to comply with the policy implementation. What is significant is that there were instances where B's resistance yielded a substantial change in the IS security policy.

This is not to say that Backhouse and Silva did not address the issue of resistance in their study of power. Indeed, they state that without resistance, episodic power cannot be identified. In fact, they state that they "could not claim that power has been exercised if users were willing to use the system" (Silva and Backhouse 2003, page 298). It is only once the system has become routinized that resistance is expected to subside. This is the heart of the process of institutionalization itself. Given the state of affairs at Millennium Bank, it is clear that this process is underway with the organization's shift towards a national standard for IS security policy.

The question of institutionalization brings to light some deficiencies in the theoretical model debuted in Figure 5.2 (pg. 107). While the relationships described are evident in the data, they do not take into account the inevitable organic stabilization that occurs with institutionalization. A social system, like an organism, tends to settle towards a homeostatic state. Social friction, in the form of resistance, will fade as the source of that resistance becomes routinized. Hence, Figure 6.4 below shows a modification to the policy-resistance model:

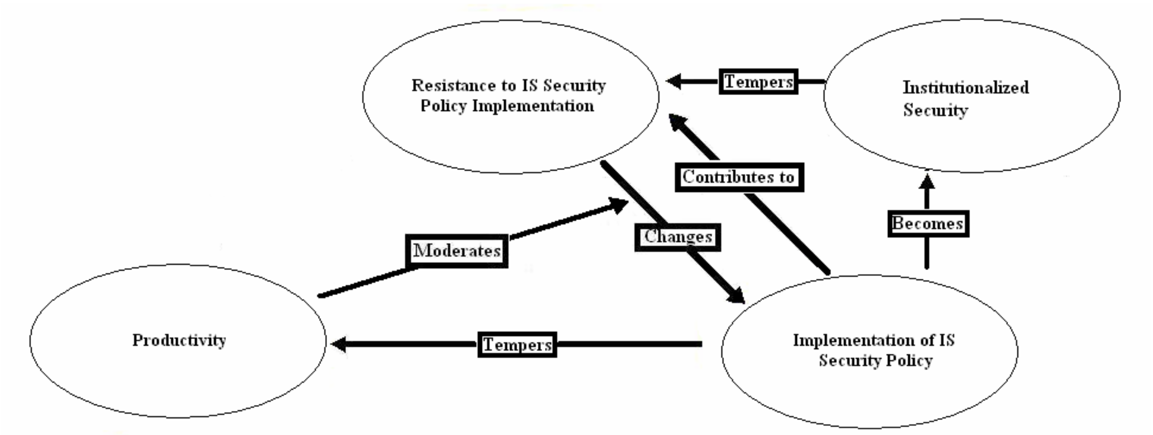

Resistance to IS Security Policy Implementation
Tempers
Institutionalized Security
Contributes to
Becomes
Moderates
Changes
Productivity
Tempers
Implementation of IS Security Policy

*Figure 6.4: Modified Policy-Resistance Model*

The modified model takes into account the institutionalization of IS security within the organization. The relationship between the implementation of IS security policy and resistance remains the same as does the tempering effect of dampened productivity. What has changed is that the transformation over time of implemented security policy into institutionalized security is noted. The verb “becomes” implies a passage of time. At the same time, institutionalized security will significantly temper the resistance to said security. The term “temper” implies that the targeted object of the relationship is reduced by the effect of the originating object.

### 6.5 Conclusion

The analysis provided in this chapter covered three major areas. The first reviewed the how data revealed insight to the research questions. While the raw data was discussed in the case chapter and the research questions were alluded to, it was important to revisit them in a specific sense. The dissertation was driven by an examination of these questions and concisely addressing them was needed. The second major area explored the contribution made by the emergent findings. The extant literature provided a context by which the findings were analyzed. The potential for future research in these emergent findings was discussed in light of the literature.

The final area of analysis discussed the implications of the findings and attempted to address the overall impact of the study. It found that the overriding theme of institutionalization was the essential point which begged an answer. How had security been institutionalized at the site under study? The analysis determined two specific implications with the findings. The first was that models of institutionalization should incorporate a feedback loop for the effects of resistance. Resistance had a profound effect on the institutionalization process at Millennium Bank. The second implication was that the shift towards a national and standardized IS security policy at the site had yet to be institutionalized. A follow-up study at the site in several years would shed light on this process.

The final chapter will recap the findings and review the entire thesis. The theoretical contributions, methodological contributions, and practical contributions shall be discussed. Potential criticisms of the research approach and design will be addressed and discussed. Finally, a summary of all future research directions will be provided.

# CHAPTER 7 Conclusion

## 7.1 Overview of the Thesis

This thesis argues that organizational power has a direct and profound impact on the development and implementation of IS Security policy. It is argued that by overlooking power relations, organizations would fall short of achieving the most effective formulation and implementation of IS Security policy. The motivation for this research stemmed from a long standing and well known issue in IS Security literature: organizations continue to lose substantial sums due to failures of IS Security.

According to the most recent FBI/CSI survey (Gordon et al. 2006), more than 52 million dollars was lost in 2006, according to the 313 respondents to the survey. Extrapolated to all organizations, the monetary losses that are a result of IS Security breaches would be exceptional. To illustrate the importance of IS Security Policy, 68% of the respondents reported that a portion of these losses was a result of insider threats. An “insider” is any individual that works within a given organ ization. These typically include employees, contractors and consultants, temporary helpers, and personnel from third-party business partners and their contractors and consultants (Schultz 2002). Almost one in ten reported that an overwhelming majority, 80 to 100%, of the losses were a result of insider threats. This evidence supports the claim that many breaches of information systems in organizations are carried out by insiders (Schultz 2002). It is these insiders that are most affected by IS Security policy.

Beyond this pragmatic aspect, there is a gap in the literature concerning power relationships and IS Security policy. This is not to say there has not been an extensive amount of research in the area of power and general IS. Indeed, Jasperson, et. al (2002) report that throughout the 1980s and 1990s, the study of power was a regular part of Management Information Systems studies. The authors sample 88 papers and conducted a metatriangulation of the literature to explore the relationships between power and information technology. Of the 88 papers, not a single paper studied security or IS security policy. This is not to say that power relationships have never been mentioned in the IS security literature (Dhillon and Backhouse 2001; Siponen 2001; Solms and Solms 2004; Karyda et al. 2005; Backhouse et al. 2006; Lapke and Dhillon 2006).

The dissertation is conducted as a two phased study whereby the first phase seeks to understand the intricacies of IS Security policy formulation and implementation. In the first phase, a conceptual framework is utilized, which is based on Katz's (1970) semantic theory. The conceptual framework provided the theoretical foundation for a case study that took place at an educational institution's Information Technology (IT) Department. In the results, it is confirmed that a disconnect exists between IS Security policy formulation and implementation. Furthermore, a significant emergent finding indicates that power relationships have a direct impact on this observed disconnect.

The second phase is an in depth interpretive case study that takes place within a large financial organization on the central east coast of the United States. This phase of the study is based on the conceptual framework of power, Circuits of Power (Clegg 2002). This conceptual framework is used to study power relationships and how they might affect the formulation and implementation of IS Security policy in the organization. The study was completed over a six month span between 2006 and 2007 and was primarily sourced by 51 semi-structured interviews (see Appendix D for the interview records).

The findings indicate that power relationships have an inescapable impact on the formulation and implementation of IS security policy. Each of the three research questions are designed to determine the degree that each of the various dimensions of the relationship between power and IS security policy are instantiated. The first question seeks to determine the ways in which power relationships within an organization have an impact on the formulation of IS Security policy. The data collected demonstrates the notable impact that power and politics have on the formulation of IS security policy. From the disempowerment of user input to the consolidation of the formulation process into a single national entity, power relationships are shown to greatly affect the way in which security policies are created.

The second research question examined the way in which power relationships within an organization have an impact on the implementation of IS Security policy. This particular research question sees power relationships manifested as resistance within the organization. There is a general perception of resistance by the bank's IS users to any implementation of security policy. Furthermore, there is actualized resistance to very controversial security policy implementations.

The final research question analyzed to what degree does the implementation of an IS Security policy has an impact on the existing power relationships within an organization. With the security policy overriding existing policies, the implementation is forcing a change in power relationships. Though very little resistance at the managerial level is noted at Millennium Bank with the inevitable power realignment, it does dampen the organizational climate. While management is aware of the need for security implementation, they are generally discontent about the loss of discretionary power. To a lesser extent, some situations of implementation yield a shift in power relations where the operational level forced a change in policy.

The emergent findings demonstrate new theoretical approaches to describing the relationship between organizational power and security policy formulation and implementation. The first new theoretical approach describes the relationship between resistance and IS security policy implementation. The theory details the interaction between the following four conceptual relationships: The implementation of IS security policy results in resistance; Resistance to the implementation of IS security policy results in a change to that policy; The implementation of IS security policy causes a negative impact on productivity; The greater the amount of negative impact on productivity causes an increase in resistance to IS security policy implementation.

The second new theoretical approach describes the effect of operational level, technically knowledgeable individuals on the formulation and implementation of IS security policy. The model described in Figure 5.3 (pg. 110) is intimately tied to the organization under study. This refers to the separation of IS security policy formulation and implementation at this particular organization. With this in mind, the primary contribution of the model is that it describes the unexpected influence of a traditionally disempowered set of employees: the technologists. This group has a significant impact on both the formulation of security policy and the way in which it was implemented or retracted.

The implications of the findings occupy the final portion of the analysis of the dissertation. Within this section, the concept of institutionalization is discussed regarding IS security policy at Millennium Bank. Considering the institutionalization of an IS is operationalized when the stabilization of its processes have reached a point where its associated practices become routine (Lamb and Kling 2003; Silva and Backhouse 2003), it is determined that IS security is not in an institutionalized state at Millennium Bank. It had been in such a state in the 20 years prior to the emerging nationalization of the IS security policy. It is now in a state of social friction as the formulation process is redefined and the new policy implementations resonate through the organization.

The remainder of this chapter discusses the contributions of the dissertation, the evaluation of the study, the research design limitations, and future research directions. The contributions are divided into the theoretical, methodological, and practical contributions, each in their own subsection.

## 7.2 Contributions

It is a consideration that "research that meets constraints only sufficiently to get published, and makes no contribution to knowledge, is not legitimate research" (Lee 2007, page 35). Given this, articulating the contributions of a dissertation should be considered one of the critical sections. This research provides several contributions that spanned the theoretical, methodological, and practical realms. These contributions are discussed in the following three subsections. The first subsection analyzes the theoretical contributions which can be described as the construction of qualitative generalizations as content of contributions (Barrett and Walsham 2004). These include concept development, theory generation, specific implications, and rich insights (Barrett and Walsham 2004). The second subsection explores the methodological contributions made by this paper. The final subsection considers the practical contributions.

### 7.2.1 Theoretical Contributions

There are several theoretical contributions made by this dissertation regarding power relationships and IS Security Policy. It must be noted however that interpretivist "theory is used in a different way than is common in positivist research; interpretive researchers are not so interested in 'falsifying' theories as in using theory more as a 'sensitizing device' to view the world in a certain way" (Klein and Myers 1999, page 75). A primary theoretical contribution involves the application of the theoretical framework based on Clegg's Circuits of Power theory. In this vein, the interpretation of Clegg's framework is a contribution in that it can be used for the study of power and politics of IS security.

A second theoretical contribution is that it filled a gap in the literature in regards to the relationship between power and IS Security. In the interpretivist paradigm, Dhillon and Backhouse (2001) noted the prevalence of power in the IS literature and speculated that this would be a future direction in IS security literature. In the same year, Trompeter (2001) touched on the potential effects of power struggles with regards to the ethics of the implementation of socio-ethical controls. Other researchers have actively called for increased empowerment of security managers in order for them to properly perform their essential duties (Siponen 2001; Solms and Solms 2004). Considering the complexities of social systems, recent exploratory works have verified that power relationships have been shown to have an impact on IS security policy (Karyda et al. 2005; Lapke and Dhillon 2006). Most recently, researchers have taken a direct look at the power and politics that international standards for IS security had emerged from (Backhouse et al. 2006).

While the topic is not vacant in the IS security literature, this dissertation has provided the next step in the study of power relationships and IS security policy. The emergence of Information Systems in organizations in the 1980s saw a wave of literature that examined the relationship between power and the implementation of Information Systems (Keen 1981; Markus 1983; Giddens 1984; Lucas 1984; Markus and Bjorn-Anderson 1987; Baronas and Louis 1988; Davis 1989; Orlikowski 1993). In a similar light, the relatively contemporary phenomenon of hyper-awareness of IS security in organizations is witnessing a return to power relationships in the IS security literature. This dissertation is laying the groundwork for a continued focus in this area.

A final theoretical contribution is the emergence of several new theoretical models that can be used in future research of IS security policy. The first is a model that described the mutually transformative relationship between the implementation of IS security policy and resistance (see Figure 5.2, pg. 107). The model describes a relationship where each entity fed on the other and how dampened productivity moderated that mutually transformative relationship. In chapter 6 (Figure 6.4, pg. 140), the model is modified to take into account the effect of institutionalization. This modification recognizes that resistance drops off significantly whence security policy becomes routinized.

A model describing the way in which power relationships affected the formulation and implementation of IS security policy is a second theoretical model that emerged from this research. The primary point to this model is the influence of the subject matter experts, or technologists, on both the formulation and implementation of IS security policy. The parties that are responsible for both formulation and implementation of IS security policy acknowledge, and to a degree expect, the technologists input but it is at an informal level.

### 7.2.2 Methodological Contributions

The methodological contribution involves the advancement of the interpretive tradition in IS research. While the interpretive paradigm has long been established in the IS literature (Walsham 2006), continuing the colonization of the IS research landscape with the interpretive approach helps to advance the field. The methodology is linked to the theory in that it illustrates how to apply the framework and analysis required to study power for researchers interested in using Clegg's (2002) Circuits of Power theory.

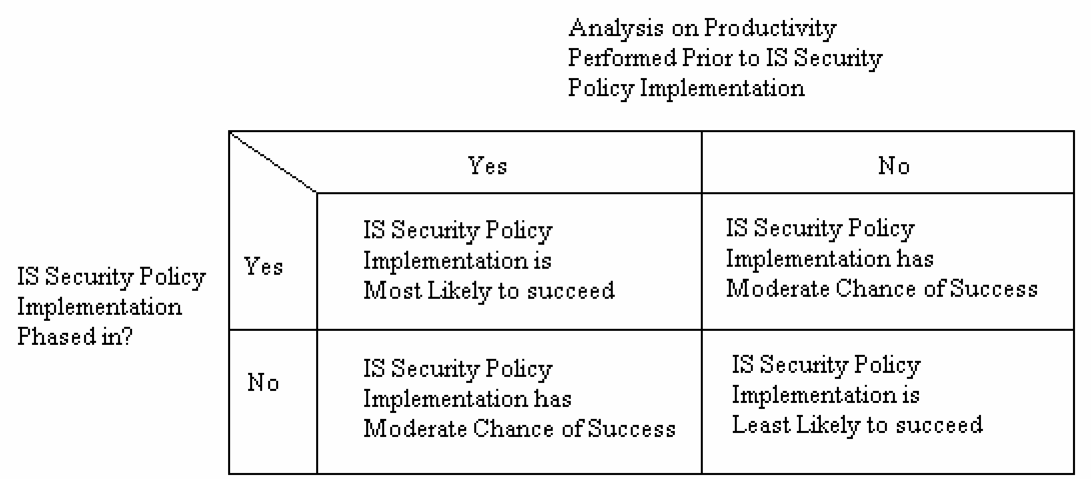
Using the first and second phases of the research as examples and the topic guide for data collection and interview (see appendix one), this research could be compared to other organizational situations. The techniques used for collecting data could be useful for other researchers studying power and politics as they relate to IS security and IS security policy. The techniques refer to the semi structured nature of data collection with the interview topic guide being based on the analytical framework constructed from Clegg's (Clegg 2002) Circuit's of Power.

In addition to the semi-structured interviews that occupied the majority of data for this study, the researcher benefited from having access to the actual security policy, as well as the minutes of the IS security policy advisory committee meetings. These methods of data collection proved invaluable in analyzing the impact of power relationships on the policy formulation and implementation. Future researchers who are doing research in sites that are experiencing nationalization or national standardization of security would find particular use of the analytical techniques (see Appendix E for the analytical tables).

### 7.2.3 Practical Contributions

The practical contribution rests in the ability of security officials to be able to best formulate and implement IS security policy. By better understanding the power relationships that impact the complex nature of regulating a social system, security officials may be best able to create and execute the most optimal possible security policy for their respective organization. The emergent findings revealed several specific areas that practitioners could find of use during the formulation or implementation process of IS security policy.

The first area that practitioners might want to address is smoothing the transition from emerging security policy to institutionalized security policy. Doing this would decrease the duration for which resistance to the implementation of the security policy is an issue. To do this, the entities responsible for policy formulation would be best suited in performing an extensive analysis on the impact a security policy might have on productivity before implementation. Understanding the relationship between actual productivity loss and security policy formulation would greatly reduce the resultant resistance. A secondary method to further reduce the organizational tension would involve phasing the security policy implementation in order to reveal unexpected effects before the organization were more profoundly impacted by resistance and actual productivity loss. Table 7.1 below indicates the likelihood of success a security practitioner might expect with the implementation of IS Security Policy given these recommendations:



| | | Analysis on Productivity Performed Prior to IS Security Policy Implementation | |
|---|---|---|---|
| | | Yes | No |
| IS Security Policy Implementation Phased in? | Yes | IS Security Policy Implementation is Most Likely to succeed | IS Security Policy Implementation has Moderate Chance of Success |
| | No | IS Security Policy Implementation has Moderate Chance of Success | IS Security Policy Implementation is Least Likely to succeed |

*Table 7.1: 2x2 Table Illustrating the Practical Application of Findings*

A second area that practitioners should address is the impact that technologists are bound to have in the IS security policy formulation and implementation process. While a healthy highly security aware organization would informally acknowledge the technologists input, it might be prudent to formalize the input of this critical group. If the formulation and implementation process follows the traditional role of managerial discretion, the organization is likely to miss out on the keen insight of this group.

## 7.3 Evaluation of the Research

As mentioned in the methodology chapter, the research is evaluated using Klein and Myer's (1999) framework for assessment of interpretive field studies. Based on this framework, the seven areas of assessment examined included examining the principle of the hermeneutic circle, contextualization, the interaction between researchers and subjects, abstraction and generalization, dialogical reasoning, multiple interpretations, and suspicion.

In performing an assessment of interpretive research, Klein and Myer's first summarize the research and indicate the research method, research site, theoretical focus, and key findings. This dissertation was conducted as a case study in a large national financial organization. The theoretical focus was the IS security policy formulation and implementation process. The key findings indicated that power relationships have a clear impact on the formulation and implementation of IS security policy. In this study, the principle of the hermeneutic circle was implied but no explicit recognition was given to it. As Klein and Myers (1999) found in the examination of the three sample articles that they evaluated, this lack of explicit recognition is due to the implication of the principle in the adherence to the other six principles.

The second principle, contextualization, was evident in the study by the way in which the case chapter was written. The data was prefaced by an in depth discussion on the context of the explicit organizational political structure. The overall security objectives and IS security policy was also discussed in detail in order to provide the necessary context.

An implicit reflection on the interaction between the researcher and the subjects, the third principle, was demonstrated throughout the case discussion. References towards the need for multiple interview sessions were described during the case chapter. While not an explicit acknowledgement of the interaction, the implication was that the researcher was approaching sensitive areas and needed to build an air of trust. As the level of comfort increased between a given subject and the researcher, the level of information sharing also showed an increase. This interaction affected the type of data collected.

The fourth principle, abstraction and generalization, indicates the relating of the "idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action" (Klein and Myers 1999, page 72). This study used Clegg's (Clegg 2002) Circuits of Power theory. From this theory, a theoretical framework was created and was used to guide the collection of data as well as the analysis of the data. Couched within the theory, the study focused on the organization processes behind the formulation and implementation of IS security policy.

The last three areas of Klein and Myers' framework all revolve around the degree of sensitivity the researcher had in performing the analysis of the data. The first, dialogical reasoning, indicates the degree to which the researcher showed sensitivity towards vetting possible contradictions between the theoretical preconceptions and the actual findings. In this study the intellectual basis of the research is made clear, but the dialogical aspect is not discussed. The second, multiple interpretations, demonstrates how the researcher shows sensitivity to differences in interpretations among the participants to the same event. The multiple interpretations actually spearheaded some of the findings. For example, the differing interpretations of management operational level employees towards the effect of security policy implementation led to the emergent finding of the realized relationship between resistance and IS security policy implementation. The third area, suspicion, relates to the researcher being sensitive to possible biases and distortions by the participants. The researcher noted the bias of the perception of security between security managers and non-security managers. One group, the security managers, indicated a pragmatic perspective that indicated an expected resistance to implementation. The second group, non-security managers, refused to acknowledge the phenomenon.

### 7.4 Criticism on Research Approach and Design

Two major areas that may be susceptible to criticism in this research are generalizability and researcher bias. While the concept of generalizability was thoroughly discussed in the methodology chapter, the bottom line is that many of the findings would simply not hold true in other organizations. Indeed, this was never the intention of this research. As it is, cases are not sampling units and should not be chosen for this reason (Yin 2003). If they are not sampling units, then they should not be analyzed or generalized in a statistical manner. While the findings may not be statistically generalizable to other organizations, they are generalizable in the analytical sense. This concept has been alluded to in both the theoretical and methodological contributions subsections.

Generalizing from description to theory is described by Yin (2003) as analytic generalization. This type of generalization means that previously developed theory is used as a template with which to compare the empirical results of the case study. He also calls this a level two inference. Quantitative research can also contribute to level two inferences but only after the statistical generalization (level one inference) is performed. Lee and Baskerville (2003) emphasize that it is important to not violate Hume's Truism when making this generalization to theory. Specifically speaking, "a theory generalized from the empirical descriptions in a particular case study has no generalizability beyond the given case" (Lee and Baskerville 2003, pg. 23).

The second major criticism that might be leveled at this research is the potential for researcher bias. This is a possibility because the researcher was employed by the organization prior to the study taking place. The organization of the primary case had strict guidelines regarding granting access to sensitive materials such as security policy and employee records. In order to be given permission to obtain access to these documents, employment was a prerequisite. This was largely because necessary criminal background checks had to be completed. Furthermore, this helped the researcher develop a rapport with the interviewees in discussing the sensitive issue of the power and politics of the organization. It is therefore believed that the risk of bias was outweighed by the benefits and outright necessity of access to the documents and employees.

### 7.5 Future Research Directions

Many of the future research directions were referenced in the fifth and sixth chapters. These stemmed from the emergent findings that arose during the analysis of the data collected during the study. The first involves the model that describes the relationship between IS security policy implementation, resistance to the implementation, worker productivity, and institutionalization (Figure 6.4, pg. 140).

There is a significant potential for future research regarding the totality of the model in how the entities interact in this model. The lingering question regarding the extent to which policy implementation actually (versus the perception of a negative impact on productivity) impacts productivity could be addressed. Furthermore, determining how an organization might mitigate both the perception and actualization of productivity loss when an IS security policy is implemented could be analyzed. A last possibility for future research involves an historical or longitudinal study that examines the way in which institutionalization impacts resistance and to what degree the IS security policy influences the institutionalization of IS security.

The second involves the model that describes the relationship between the technical group and managerial groups that are responsible for the formulation and implementation of IS security policy. While the relationship between technologists and management has been studied extensively in general IS research, there is very little in the way of IS Security research that explores this phenomenon. Some questions that could be answered include: In what ways do technologists communicate there IS security policy suggestions in light of their position of power? In situations where technologists are left out of the loop, is the security of the firm left in a less effective state than where technologists are openly welcomed by the management staff?

Another mitigating factor that could be explored in light the technological influence could be the changing of influence that the technical groups have as executives and managers trend towards increasing technical awareness. As newer generations of individuals with a more technocentric background begin to fill executive roles within organizations, it is likely that this technical gap between management and technologists will shrink. This would have a clear impact on power relationships within organizations as the reliance on technologists would be less profound.

# List of References

# List of References

Adler, P. and P. Adler (1994). Observational Techniques. Handbook of Qualitative Research. N. Denzin and Y. Lincoln. Thousand Oaks, CA, Sage**:** 377-392.

Albrechsten, E. (2007). "A qualitative study of users' view on information security." Computers and Security **26**(4): 276-289.

Allen, D., T. Kern and D. Mattison (2002). "Culture, power and politics in ICT outsourcing in higher education institutions." European Journal of Information Systems **11**: 159-173.

Anderson, P. (1990). "A Theory of Computer Semiotics: Semiotic Approaches to Construction and Assessment of Computer Systems." Computational Linguistics **18**(4): 555-562.

Anderson, R. (1996). A Security Policy Model for Clinical Information Systems. IEEE Symposium on Security and Privacy.

Anonymous (2007). Oxford English Dictionary. J. Simpson. Oxford, Oxford University Press.

Backhouse, J. (1992). The use of semantic analysis in the development of information systems. Department of IS. London, London School of Economics.

Backhouse, J., C. Hsu and L. Silva (2006). "Circuits of power in creating de jure standards : shaping an international information systems security standard." MIS Quarterly **30**: 413-438.

Barley, S. (1990). "The alignment of technology and structure through roles and networks." Administrative Science Quarterly **35**(1): 61-104.

Baronas, A. and M. Louis (1988). "Restoring a Sense of Control During Implementation: How User Involvement Leads to System Acceptance." MIS Quarterly **12**(1): 329-336.

Barrett, M. and G. Walsham (1995). "Using IT to Support Business Innovation: A Case Study of the London Insurance Market." Scandinavian Journal of Information Systems **7**(2): 3-22.

Barrett, M. and G. Walsham (2004). Making Contributions from Interpretive Case Studies: Examining Processes of Construction and Use. Information Systems Research: Relevant Theory and Informed Practice. B. Kaplan, D. Truex, D. Wastell, D. Wood-Harper and J. DeGross, Springer**:** 293-314.

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development." ACM Computing Surveys **35**(4): 375 - 414.

Baskerville, R. and M. Siponen (2002). "An information security meta-policy for emergent organizations." Logistics Information Management **15**(5/6): 337-346.

Beckhard, R. (1969). Organization Development: Strategies and Models. Reading, MA, Addison-Wesley.

Bequai, A. (1998). "Employee Abuses in Cyberspace: Management's Legal Quagmire." Computers & Security **17**: 667-670.

Berg, A. (1995). "Cracking a Social Engineer." Computers & Security **14**(8): 700.

Besnard, D. and B. Arief (2004). "Computer Security Impaired by Legitimate Users." Computers & Security **23**: 253-264.

Burrell, G. and G. Morgan (1979). Sociological Paradigms and Organizational Analysis. London, Heinemann Education Books, Ltd.

Callon, M. (1986). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. Power, Action and Belief. J. Law. London, Routledge**:** 196 233.

Campbell, D. and J. Stanley (1966). Experimental and Quasi-experimental Designs for Research. Chicago, Rand McNally.

Carroll, J. (1996). Computer Security. Newton, MA, Butterworth-Heinemann.

Cavaye, A. and J. Christiansen (1996). "Understanding IS implementation by estimating power of subunits." European Journal of Information Systems **5**: 222-232.

Ceraolo, J. P. (1996). "Penetration testing through social engineering." Information Systems Security **4**(4).

Cho, S. and H. Park (2003). "Efficient anomaly detection by modeling privilege flows using hidden Markov model." Computers & Security **22**(1): 45-55.

Clegg, S. (2002). Frameworks of Power. Thousand Oaks, CA, Sage Publications.

Coyne, J. and N. Kluksdahl (1994). “Mainstreaming” Automated Information Systems Security Engineering (A Case Study in Security Run Amok). ACM Conference. Fairfax, VA.

Damianides, M. (2005). "Sarbanes–Oxley And It Governance: New Guidance On It Control And Compliance." Information Systems Management: 77-85.

David, J. (2002). "Policy Enforcement in the Workplace." Computers & Security **21**(6): 506-513.

Davis, F. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." MIS Quarterly **13**(3): 319-340.

Denzin, N. and Y. Lincoln (1994). Introduction: Entering the Field of Qualitative Research. Handbook of Qualitative Research. N. Denzin and Y. Lincoln. Thousand Oaks, CA, Sage**:** 1-18.

Dhillon, G. (2004). "Dimensions of power and IS implementation." Information and Management **41**(5): 635-644.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, NJ, John Wiley & Sons.

Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM **43**(7): 125-128.

Dhillon, G. and J. Backhouse (2001). "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives." Information Systems Journal **11**: 127-153.

Dhillon, G. and J. May (2006). Interpreting Security in Human-Computer Interactions: A Semiotic Analysis. Human-Computer Interaction and Management Information Systems: Foundations. P. Zhang and D. Galletta. Armonk, NY, M.E. Sharp.

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

Doherty, N. and H. Fulford (2005). "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis." Information Resources Management Journal **18**(4): 21-39.

Doherty, N. and H. Fulford (2006). "Aligning the information security policy with the strategic information systems plan." Computers & Security **25**: 55-63.

Earl, M. (1993). "Experiences in Strategic Information Systems Planning." MIS Quarterly **17**(1): 1-24.

Elkjaer, B., P. Flensburg, J. Mouritsen and H. Willmott (1991). "The Commodification of Expertise: The Case of Systems Development Consulting." Accounting, Management and Information Technologies **1**(2): 139-156.

Eysenck, H. and S. Eysenck (1965). "The Eysenck Personality Inventory." British Journal of Educational Studies **14**(1): 24.

Fazio, R. and C. Williams (1986). "Attitude accessibility as a moderator of attitude-perception and attitude-behavior relation: An investigation of the 1984 presidential election." Journal of Personality and Social Psychology **51**: 505-514.

Ferris, J. (1994). "Using Standards as a Security Policy Tool." ACM Standard View **2**(2): 73-77.

Foley, S. (1997). "Building Chinese walls in standard unix." Computers & Security **16**(6): 551-563.

Fontana and Frey (1994). Interviewing: The Art of Science. Handbook of Qualitative Research. N. Denzin and Y. Lincoln. Thousand Oaks, CA, Sage**:** 361-376.

Foucault, M. (1977). Discipline and Punish: The Birth of the Prison, Vintage.

Furnell, S., P. Dowland, H. Illingworth and P. Reynolds (2000). "Authentication and Supervision: A Survey of User Attitudes." Computers & Security **19**(6): 529-539.

Galliers, B. (1999). "Towards the integration of e-business, knowledge management and policy considerations within an information systems strategy framework." Journal of Strategic Information Systems **8**: 229-234.

Gerber, M. and R. Von Solm (2006). "Management of risk in the information age." Computers & Security **24**: 16-30.

Giddens, A. (1984). The Constitution of Society: Outline of the Theory of Structure. Berkeley, CA, University of California Press.

Glasgow, J. and G. Macewen (1992). "A Logic for Reasoning about Security." ACM Transactions on Computer Systems **10**(3): 226-264.

Gliner, J. and G. Morgan (2000). Research Methods in Applied Settings An Integrated Approach to Design and Analysis. New Jersey, Lawrence Erlbaum Associates.

Gordon, L., M. Loeb, W. Lucyshyn and R. Richardson (2006). "2006 CSI/FBI Computer Crime and Security Survey." Computer and Security Institute **11**(1): 1-27.

Gritzalis, D. (1997). "A baseline security policy for distributed healthcare information systems." Computers & Security **16**(8): 709-719.

Guba, E. and Y. Lincoln (1994). Competing paradigms in qualitative research. Handbook of Qualitative Research. N. Denzin and Y. Lincoln. Thousand Oaks, CA, Sage**:** 105-117.

Hambrick, D. (1980). "Operationalizing the concept of business-level strategy in research." The Academy of Management Review **5**(4): 567.

Han, S. and S. Cho (2003). "Detecting intrusion with rule-based integration of multiple models." Computers & Security **22**(7): 613-623.

Harris, B. and R. Hunt (1999). "Firewall Certification." Computers & Security **18**(2): 165-177.

Haworth and Pietron (2006). "Sarbanes–Oxley: Achieving Compliance By Starting With Iso 17799." Information Systems Management: 73-87.

Hersey, P., K. Blanchard and D. Johnson (2001). Management of Organizational Behavior. Upper Saddle River, NJ, Prentice Hall.

Hirschheim, R. and H. Klein (1994). "Realizing emancipatory principles in information systems development: The case for ETHICS." MIS Quarterly **18**(1): 83-109.

Hirschheim, R., H. Klein and Lyttenin (1995). Information Systems Development and Data Modeling, Conceptual and Philosophical Foundations. Cambridge, University Press.

Hodder, I. (1994). The Interpretation of Documents and Material Culture. Handbook of Qualitative Research. N. Denzin and Y. Lincoln. Thousand Oaks, Sage**:** 393-402.

Hoffman, L., F. Ali, S. Heckler and A. Huybrechts (1994). "Cryptography policy." Communications of the ACM **37**(9): 109-117.

Holmström, U. (1999). User-Centered Design of Security Software. Human Factors in Telecommunication. Copenhagen, Denmark.

Hone, K. and J. Eloff (2002). "Information security policy: What do international information security standards say?" Computers & Security **5**(1): 402-409.

Howcroft and Trauth (2005). Handbook of Critical Information Systems Research. Northampton, Edward Elgar Publishing, Inc.

Huberman, A. and M. Miles (1994). Data Management and Analysis Methods. Handbook of Qualitative Research. N. Denzin and Y. Lincoln. Thousand Oaks, Sage**:** 429-444.

Huston, T. (2001). "Security Issues for Implementation of E-Medical Records." Communications of the ACM **44**(9).

Jagatic, T., N. Johnson, M. Jakobsson and F. Menczer (2007). "Social Phishing." Communications of the ACM **50**(10).

Jarvenpeena and Tiller (1999). "Integrating market, technology, and policy opportunities in e-business strategy." Journal of Strategic Information Systems **8**: 235-249.

Jarvenpeena, S. (1991). "Executive Involvement and Participation in the Management of Information Technology." MIS Quarterly **15**(2): 205.

Jasperson, J., et al. (2002). "Review: Power and Information Technology Research: A Metatriangulation Review." MIS Quarterly **26**(4): 397-459.

Jones, M., W. Orlikowski and K. Munir (2004). Strucuration Theory and Information Systems: A Critical Reappraisal. Social Theory And Philosophy For Information Systems. J. Mingers and L. Willcocks. Hoboken, NJ, Wiley**:** 297-328.

Joshi, J., A. Ghafoor and S. E (2001). "Digital Government Security Infrastructure Design Challenges." Computer **34**(2): 66-72.

Joshi, K. (1991). "A Model of Users' Perspective on Change: The Case of Information Systems Technology Implementation." MIS Quarterly **15**(2): 229-242.

Kamara, S., et al. (2003). "Analysis of Vulnerabilities in Internet Firewalls." Computers & Security **22**(3): 214-232.

Kaplan, B. and J. Maxwell (1994). Qualitative Research Methods for Evaluating Computer Information Systems. Evaluating Health Care Information Systems: Methods and Applications. J. Anderson, C. Aydin and S. Jay. Thousand Oaks, CA, Sage**:** 45-68.

Karahana, E., D. Straub and N. Chervany (1999). "Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs." MIS Quarterly **23**(2): 183-213.

Karyda, M., E. Kiountouzis and S. Kokolakis (2005). "Information systems security policies: a contextual perspective." Computers & Security **24**: 246-260.

Katz, J. (1970). Semantic Theory. New York, Harper and Row.

Keen, P. (1981). "Information Systems and Organizational Change." Communications of the ACM **24**(1): 24-33.

Kettinger, W. and V. Grover (1995). "Special section: toward a theory of business process change management." Journal of Management Information Systems **12**(1): 9-30.

King, W. (1978). "Strategic Planning for Information Systems." MIS Quarterly **2**(1): 27-37.

Klein, H. and M. Myers (1999). "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems " MIS Quarterly **23**(1): 67-93.

Kühnhauser, W. (1999). "Policy Groups." Computers & Security **18**(4): 351-363.

Lamb, R. and R. Kling (2003). "Reconceptualizing Users as Social Actors In Information Systems Research." MIS Quarterly **27**(2): 197-235.

Land, F. (1976). "Evaluation of systems goals in determining a design strategy for a computer based information system." The Computer Journal **19**(4): 290-294.

Landau, S., et al. (1994). "Crypto Policy Perspectives." Communications of the ACM **37**(8): 115-121.

Lapke, M. and G. Dhillon (2006). A Semantic Analysis of Information Systems Security Policy Formulation and Implementation: A Case Study. . 12th Annual America's Conference for Information Systems. , Acapulco, Mexico.

Lederer, A. and H. Salmela (1996). "Toward a theory of strategic information systems planning." Journal of Strategic Information Systems **5**: 237-253.

Lee, A. (2004). Thinking about Social Theory and Philosophy for Information Systems. Social Theory And Philosophy For Information Systems. J. Mingers and L. Willcocks. Hoboken, NJ, Wiley**:** 1-26.

Lee, A. (2007). "Crafting a Paper for Publication." Communications of the Association for Information Systems **20**: 33-40.

Lee, A. and R. Baskerville (2003). "Generalizing Generalizability in Information Systems Research." information Systems Research **14**(3): 221-243.

Leontiades, M. (1982). "The Confusing Words of Business Policy." The Academy of Management Review **7**(1): 45.

Liebenau, J. and J. Backhouse (1990). Understanding Information: An Introduction. London, Macmillan.

Lin, A. and L. Silva (2005). "The social and political construction of technological frames." European Journal of Information Systems **14**: 49-59.

Lin, C. (2001). "Hierarchical key assignment without public-key cryptography." Computers & Security **20**(7): 612-619.

Lind, M. and R. Zmud (1991). "The Influence of a Convergence in Understanding between Technology Providers and Users on Information Technology Innovativeness." Organization Science **2**(2): 195-217.

Loch, K., H. Carr and M. Warkentin (1992). "Threats to Information Systems: Today's Reality, Yesterday's Understanding." MIS Quarterly **16**(2): 173.

Lucas, H. C. (1984). "Organizational power and the information services department." Communications of the ACM **27**(1): 1218-1226.

Lukes, S. (1974). Power: A Radical View. London, Macmillan.

Markus, M. (1983). "Power, Politics, and MIS Implementation." Communications of the ACM **26**(6): 430.

Markus, M. and N. Bjorn-Anderson (1987). "Power over users: Its exercise by system professionals." Communications of the ACM **26**(6): 430-444.

Mattia, A. and G. Dhillon (2003). Applying Double Loop Learning to Interpret Implications for Information Systems Security Design. IEEE International Conference on Systems, Man and Cybernetics, 2003. .

Mintzberg, H. (1983). Structures in Fives: Designing Effective Organizations. Englewood Cliffs, NJ, Prentice Hall.

Mintzberg, H. (1992). "Cycles of Organizational Change." Strategic Management Journal **13**(Special Issue): 39-59.

Mintzberg, H., J. Lampel, J. Quinn and S. Goshal (2003). The Strategy Process, Prentice Hall.

Morris, C. (1970). Foundations of the Unity Of Science: Toward an International Encyclopedia of Unified Science. Chicago, University of Chicago Press.

Mumby, D. (2005). "Theorizing Resistance In Organization Studies A Dialectical Approach." Management Communication Quarterly **19**(1): 19.

Mumford, E. (1983). Designing Human Systems: the ETHICS method.

Myers, M. (1994). Quality in Qualitative Research in Information Systems. 5th Australasian Conference on Information Systems.

Nandhakumar, J. and M. Jones (1993). Structured Development? A Structurational Analysis of the Development of an Executive Information System. IFIP WG8.2 Working Group on Information Systems Development: Human, Social, and Organizational Aspects: Human, Organizational, and Social Dimensions of Information Systems Development.

Nelson, K. and J. Nelson (2003). The Need for a Strategic Ontology. International Conference for Information Systems. J. King and K. Lyttenin. Seattle, WA.

Newman, M. and D. Robey (1992). "User Involvement as an Interaction Process: A Case Study." Information Systems Research **1**(1): 321-332.

Niven, J. (1990). "Alternative reinforcement increases resistance to change: Operant or Pavlovian processses? ." Journal of the Experimental Analysis of Behavior **53**: 359-379.

Olson, M. and N. Chervaney (1980). "The Relationship between Organizational Characteristics and the Structure of the Information Services Function." MIS Quarterly **4**(2): 57-68.

Orlikowski, W. (1993). "CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development." MIS Quarterly **17**(3): 309-340.

Orlikowski, W. and S. Barley (2001). "Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? ." MIS Quarterly **25**(2): 145-165.

Orlikowski, W. and J. Baroudi (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." Information Systems Research **2**(1): 1-28.

Orlikowski, W. and D. Hofman (1997). "An Improvisational Model for Change Management: The Case of Groupware Technologies." Sloan Management Review **38**(2): 11-21.

Ostroff, C., A. Kinkicki and M. Tamkins (2003). Organizational Culture and Climate. Handbook of Psychology. W. Burman, D. Ligen and R. Klimoski. New York, Wiley and Sons. **12:** 565-593.

Peppard, J. (2007). "The conundrum of IT management." European Journal of Information Systems **16**(4): 336-345.

Pettigrew, A. (1972). "Information Control as a Power Resource." Sociology **6**(2): 187-204.

Pfleeger, C. (1999). Security in Computing, Prentice-Hall.

Porter, M. (1979). "How competitive forces shape strategy." Harvard Business Review **57**(3): 87-94.

Posthumus, S. and R. Solms (2004). "A framework for the governance of information security." Computers & Security **23**(8): 638-646.

Rees, J., S. Subhajyoti and E. Spafford (2003). "PFIRES: A Policy Framework for Information Security." Communications of the ACM **46**(7): 101-106.

Reich, B. and I. Benbasat (2000). "Factors that influence the social dimension of alignment between business and information technology objectives." MIS Quarterly **24**(1): 81-113.

Robinson, S. and R. Bennett (1995). "A Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Stud." The Academy of Management Journal **38**(2): 555-572.

Rogers, L. (2004). "Principles of Survivability and Information Assurance." Software Engineering Institute.

Sandhu, R. (1992). "Lattice-Based Enforcement of Chinese Walls." Computers & Security **11**(8): 753-763.

Schein, E. (1992). Organizational Culture and Leadership, Jossey-Bass.

Schön, D. (1983). The Reflective Practitioner. How professionals think in action, Temple Smith.

Schultz, E. (2002). "A framework for understanding and predicting insider attacks." Computers & Security **21**(6): 526-531.

Schultz, E. (2004). "The case for one-time credentials." Computers & Security **23**(6): 441-442.

Schultz, E. (2004). "Security training and awareness fitting a square peg in a round hole." Computers & Security **23**(1).

Schultze, U. and D. Leidner (2002). "Studying Knowledge Management In Information Systems Research: Discourses And Theoretical Assumptions." MIS Quarterly **26**(3): 213-242.

Scott, J. (1985). Weapons of the Weak: Everyday Forms of Peasant Resistance. New Haven, Yale University Press.

Segers, A. and V. Grover (1999). "Profiles of Strategic Information Systems Planning." Information Systems Research **10**(3): 199-232.

Silva, L. (1997). Power and Politics in the adoption of information systems by organisations: The case of a research centre in Latin America. Information Systems. London, London School of Economics and Political Science. **Doctor of Philosophy**.

Silva, L. and J. Backhouse (1997). Becoming part of the furniture: The Institutionalization of Information Systems. Information Systems and Qualitative Research. A. Lee, J. Liebenau and J. DeGross. London, Chapman and Hall.

Silva, L. and J. Backhouse (2003). "The circuits-of-power framework for studying power in institutionalization of information systems." Journal of the Association for Information Systems **4**: 294-336.

Siponen, M. (2000). "A conceptual foundation for organizational information security awareness." Information Management & Computer Security **8**(1): 31-41.

Siponen, M. (2001). "An analysis of the traditional IS security approaches: implications for research and practice." Information Management & Computer Security **8**(1): 31.

Skinner, B. F. (1938). The behavior of organisms: An experimental analysis. Cambridge, MA, Appleton-Century-Crofts.

Smyth, J. (1989). "Collegiality as a Counter Discourse to the Intrusion of Corporate Management into Higher Education." Journal of Tertiary Education Administration **11**(2): 143-155.

Solms, B. and R. Solms (2004). "The 10 deadly sins of information security management." Computers & Security **23**: 371-376.

Solms, R. and B. Solms (2004). "From policies to culture." Computers & Security **23**(4): 275-279.

Spinellis, D., et al. (1999). "Trusted third party services for deploying secure telemedical applications over the WWW." Computers & Security **18**(7): 627-639.

Stamper, R. (1973). Information in Business and Administrative Systems. New York, Halstead Press.

Sterman, J. (2000). Business Dynamics: Systems Thinking and Modeling for a Complex World. New York, Irwin McGraw-Hill.

Straub, D. (1990). "Effective IS Security: An Empirical Study." Information Systems Research **1**(3): 255-276.

Straub, D. and R. Welke (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making." MIS Quarterly **22**(4): 441-469.

Svenson, A., U. Mazzucato, P. Gordon and W. Starbuck (1966). "Forum: Exchanges on cases and policy courses." Academy of Management Journal **9**(4): 344-361.

Tan, F. and M. G. Hunter (2002). "The Repertory Grid Technique: A Method for the Study of Cognition In Information Systems." MIS Quarterly **26**(1): 39-57.

Trček, D. (2003). "An integral framework for information systems security management." Computers & Security **22**(4): 337-360.

Trompeter, C. and J. Eloff (2001). "A Framework for the Implementation of Socio-ethical Controls in Information Security." Computers & Security **20**(5): 384-391.

Ulrich, W. (2001). "A Philosophical Staircase for Information Systems Definition, Design, and Development." Journal of Information Technology Theory and Application **3**: 55-84.

Venkatraman, N., J. Henderson and S. Oldach (1993). "Continuous strategic alignment: exploiting information technology capabilities for competitive success." European Management Journal **11**(2): 139-149.

Waddell, D. and A. Sohal (1998). "Resistance: a constructive tool for change management." Management Decision **36**(8): 543-548.

Walsham, G. (1993). Interpreting Information Systems in Organizations. Chichester, UK, Wiley.

Walsham, G. (1995). "The Emergence of Interpretivism in IS Research." Information Systems Research **6**(4): 376-394.

Walsham, G. (2006). "Doing Interpretive Research." European Journal of Information Systems **15**(3): 320-330.

Ward, P. and C. Smith (2001). "The Development of Access Control Policies for Information Technology Systems." Computers & Security **21**(4): 356-371.

White, K. and R. Leifer (1986). "Information Systems Development Success: Perspectives from Project Team Participants." MIS Quarterly **10**(3): 215-223.

Whitman, M., A. Townsend and R. Aalberts (2001). Information Systems Security and the Need for Policy. Information Security Management: Global Challenges in the New Millennium. G. Dhillon**:** 9-18.

Willcocks, L. (2004). Foucault, Power/Knowledge and Information Systems: Reconstructing the Present. Social Theory And Philosophy For Information Systems. J. Mingers and L. Willcocks. Hoboken, NJ, Wiley**:** 238-296.

Willcocks, L. and T. Kern (1998). "IT outsourcing as strategic partnering: the case of the UK Inland Revenue." European Journal of Information Systems **7**(1): 29-45.

Willison, R. (2002). Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank. Department of IS. London, London School of Economics. **Ph.D.**

Wilson, M. and D. Howcroft (2002). "Re-conceptualising failure: social shaping meets IS research." European Journal of Information Systems **11**(4): 236-250.

Wool, A. (2004). "The use and usability of direction-based filtering in firewalls." Computers & Security **23**: 459-468.

Yin, R. (2003). Case Study Research Design and Methods. Thousand Oaks, CA, Sage Publications.

Zmud, R. and J. Cox (1979). "The Implementation Process: A Change Approach." MIS Quarterly **3**(2): 35-43.

Zuboff, S. (1989). In the Age of the Smart Machine: The Future of Work and Power Basic Books.

# Appendix A

Topic Guide

1. Describe your job at this organization.
2. Who do you consider to be powerful within this organization?
3. What are the characteristics of the day to day social interactions between you and your superiors?
4. What are the characteristics of the day to day social interactions between you and those that work for you?
5. Have you ever found fluctuations in your productivity due to intentional or unintentional resistance to security related management directives?
6. Have you ever found fluctuations in your subordinate's productivity security related directives have been imposed?
7. To your knowledge, has a sentiment of resistance to new security measures ever been apparent in the organization?
8. If there has been any kind of resistance to new security measures, has this resistance yielded any noticeable impact in the organization?
9. Have you ever resisted (verbally or by action) any security measures imposed by the organization?
10. What are you thoughts on the explicit organizational structures (from mid-level management to executive management) at this organization?
11. In the instances when resistance to security measures has come about, what kind of reaction has there been from those supervisors in the organization?
12. In the instances when resistance to security measures has come about, have you noticed any informal compromises and agreements come about that directly deal with the security issue?
13. Has resistance to security measures been discussed at an organizational level (i.e. via security awareness programs)? If so, what was your reaction to this discussion?
14. Are you aware of any specific consequences to resistance to new security measures by employees?
15. If there are implicit or explicit consequences for resistance, are they enforced?
16. If you are given a new security directive that might negatively impact your productivity, have you ever found a way around the new security directive?
17. Has your immediate superior ever given you the go ahead to ignore particular security measures in order to avoid "making your job harder than it needs to be?"

# Appendix B

Figures

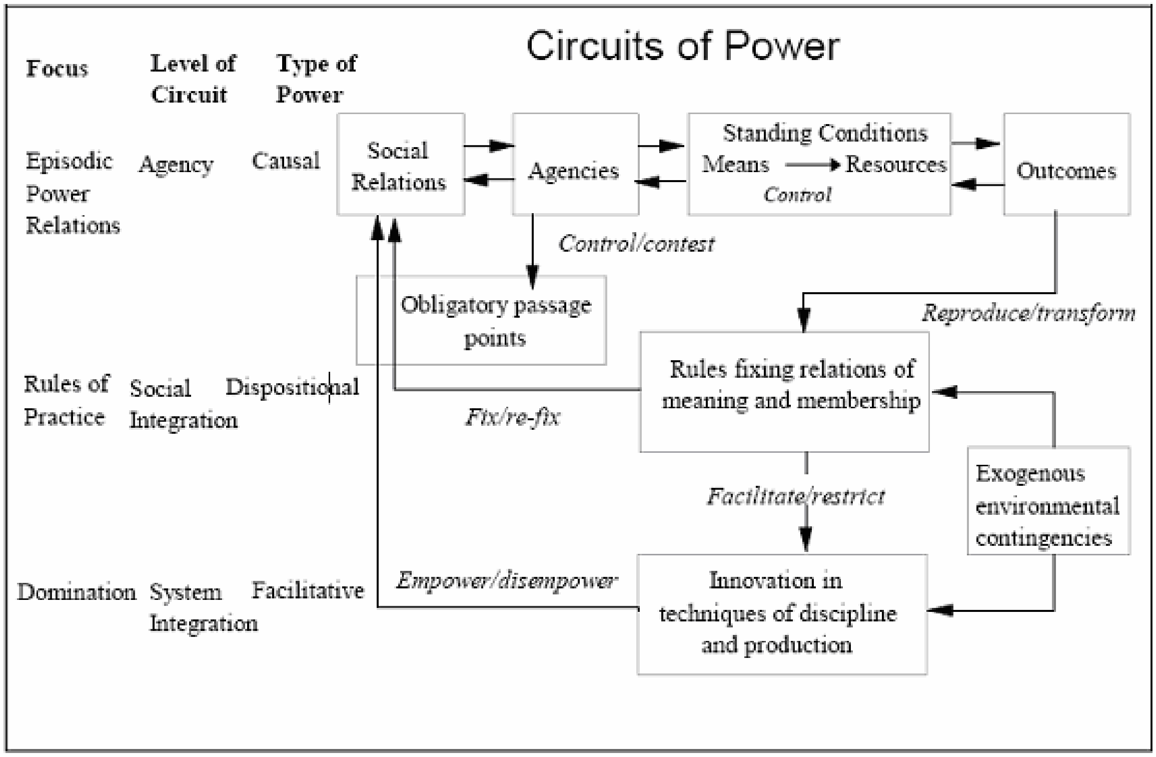


*Figure 4.1: Circuits of Power*

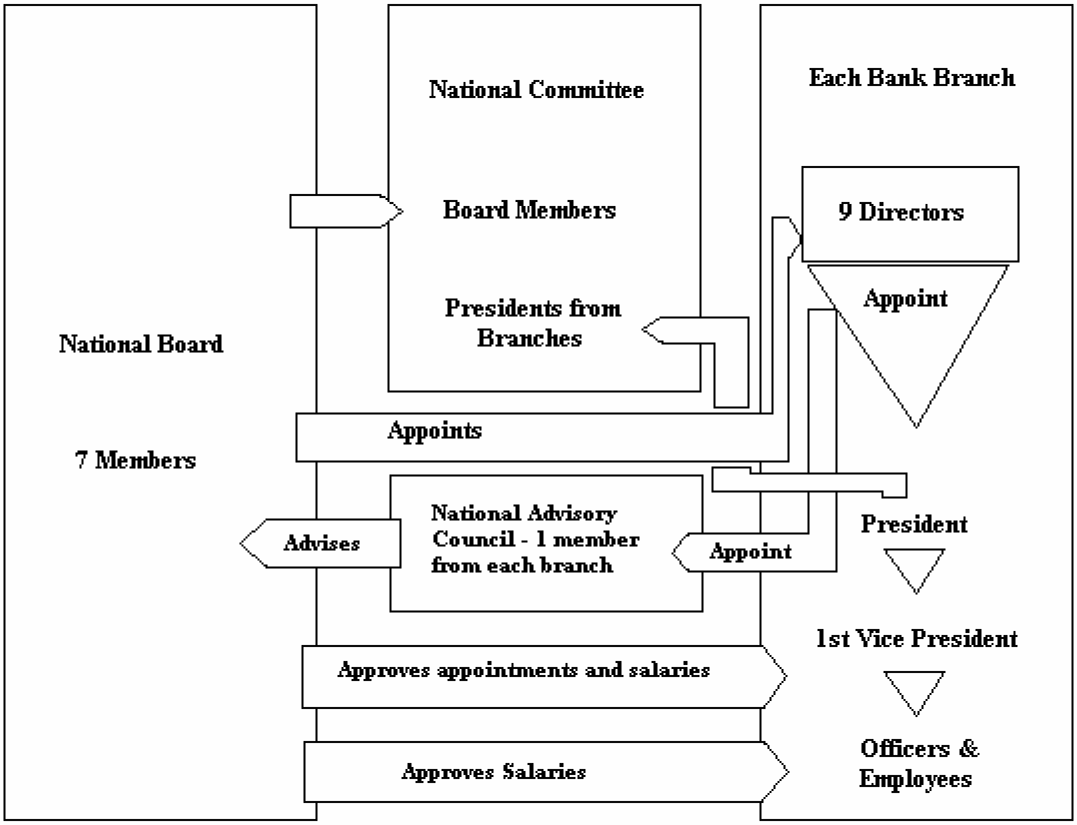


*Figure 5.1: Organization of Millennium Bank*

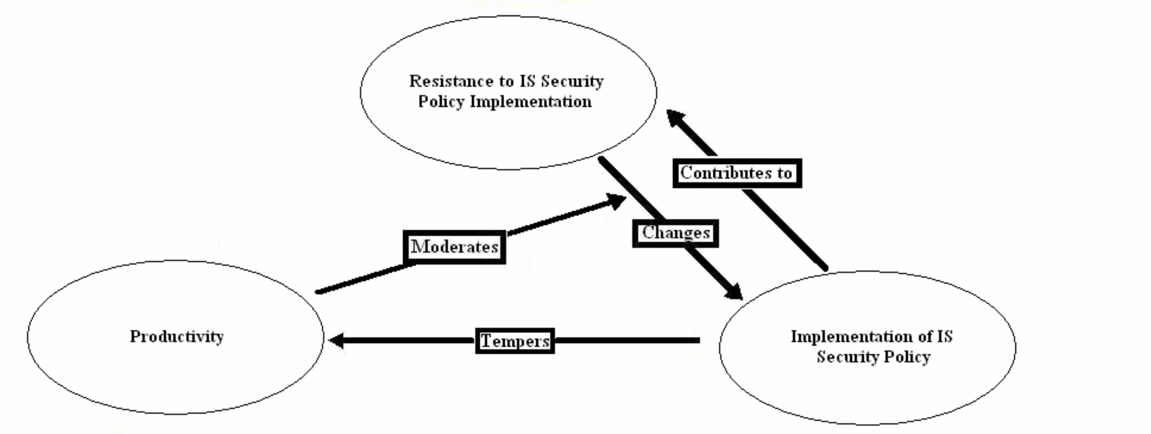

Resistance to IS Security Policy Implementation
Contributes to
Moderates
Changes
Productivity
Tempers
Implementation of IS Security Policy

*Figure 5.2: The relationship between IS security policy and resistance*

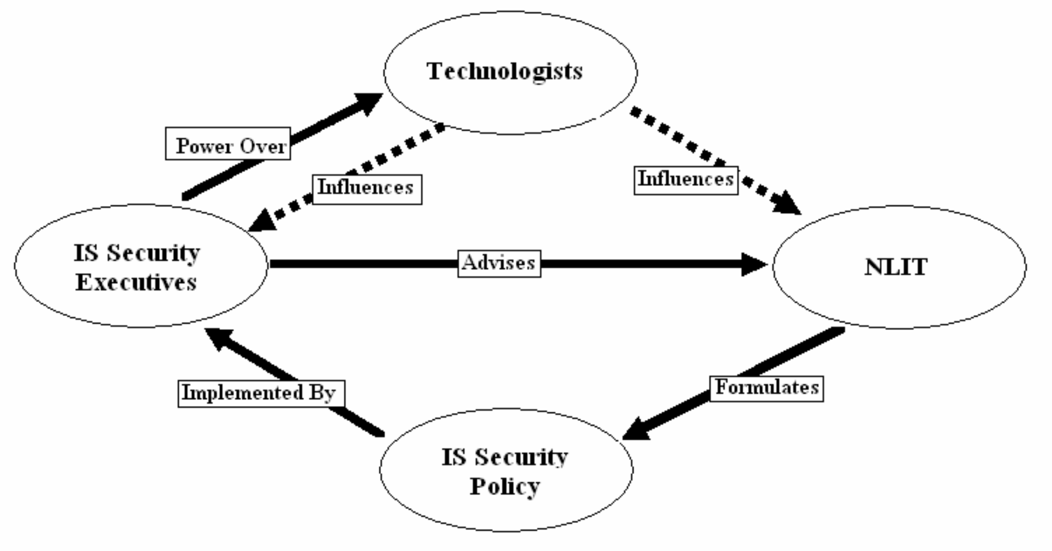


*Figure 5.3: The power brokers impact on IS security policy*

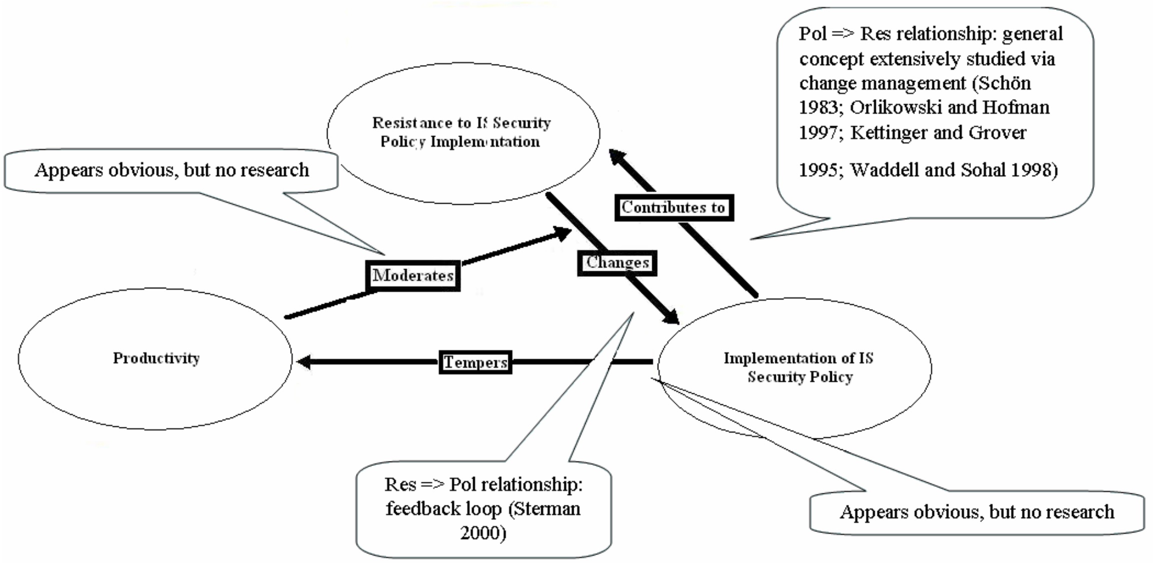

Pol => Res relationship: general concept extensively studied via change management (Schön 1983; Orlikowski and Hofman 1997; Kettinger and Grover 1995; Waddell and Sohal 1998)
Resistance to IS Security Policy Implementation
Appears obvious, but no research
Contributes to
Changes
Moderates
Productivity
Tempers
Implementation of IS Security Policy
Res => Pol relationship: feedback loop (Sterman 2000)
Appears obvious, but no research

*Figure 6.1: Analysis of the Relationships in the Policy Resistance Model*

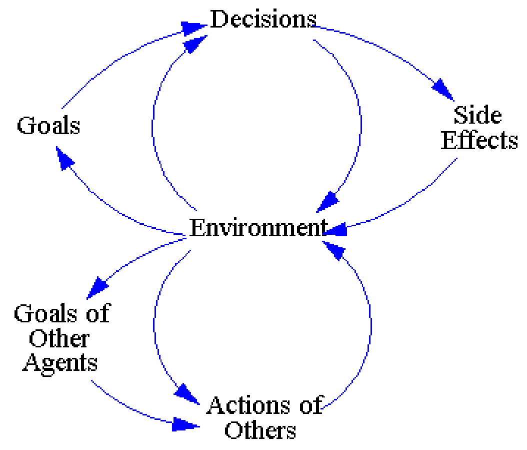


*Figure 6.2: Dynamic System Feedback Model*

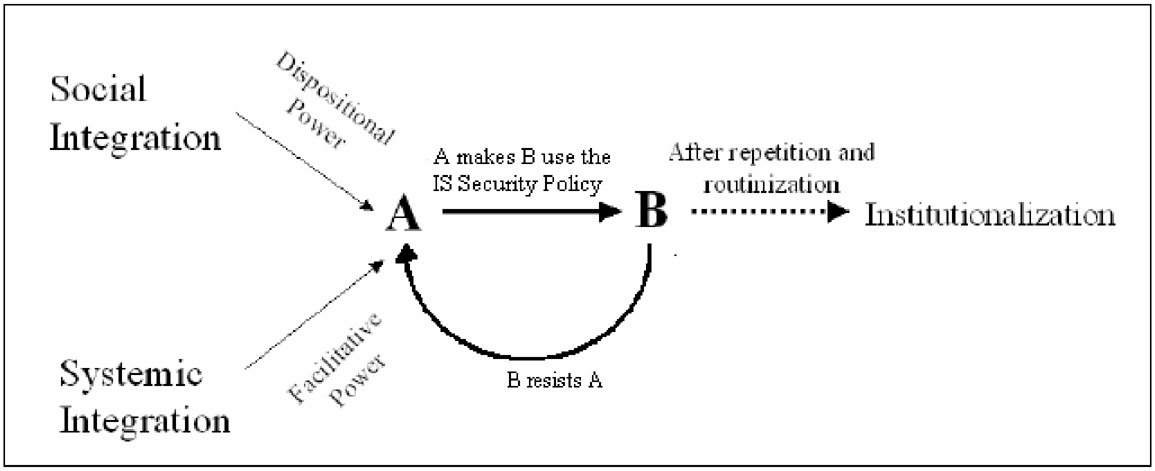


*Figure 6.3: Modified Model of Institutionalization*

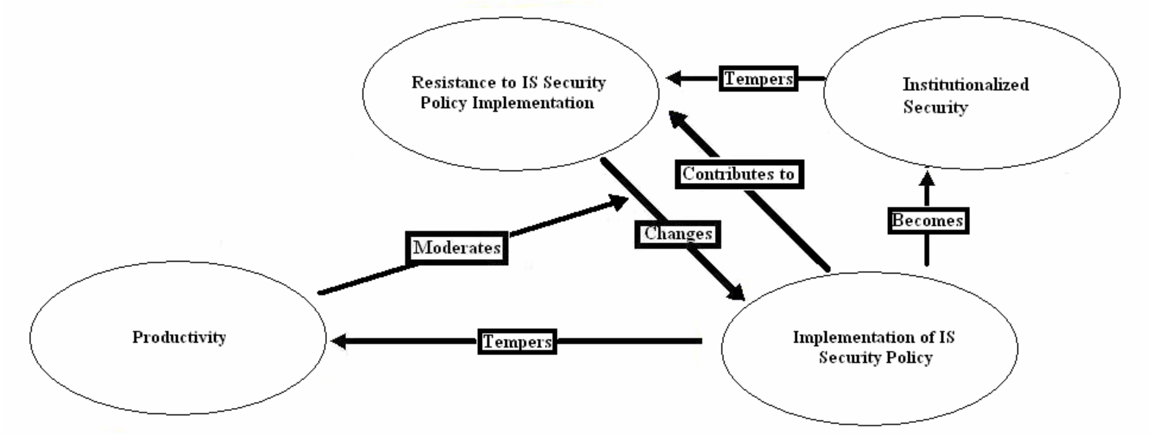

Resistance to IS Security Policy Implementation
Tempers
Institutionalized Security
Contributes to
Becomes
Moderates
Changes
Productivity
Tempers
Implementation of IS Security Policy

*Figure 6.4: Modified Policy-Resistance Model*

# Appendix C

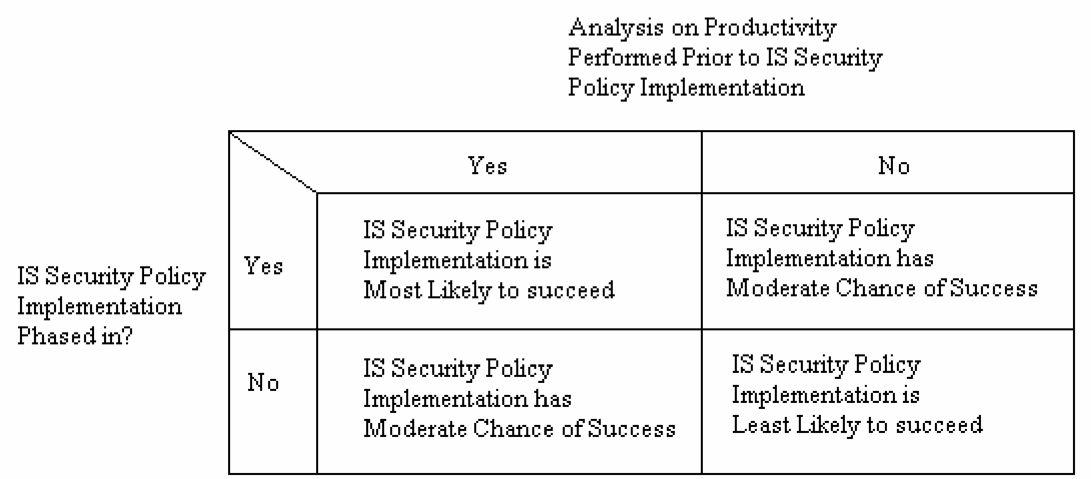
## Tables

| Semantic Element | Description and seminal works | IS Security Policy Formulation | IS Security Policy Implementation |
|---|---|---|---|
| Denotative Descriptions<br>• Designation<br>• Facts<br>• Evidence<br>• Forecasts | This semantic element is simply a statement of something that exists. (Stamper, 1973)<br>The nature of the environment in which the organism operates. (Morris, 1970). | What are the known current vulnerabilities of the system in question?<br>How technically secure is the IS in its current state?<br>How physically (and socially) secure is the IS in its current state?<br>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?<br>Is the security policy required reading for all the users of the system?<br>Are the security policy procedures actually followed by the IS users? |
| Affective Descriptions<br>• Appraisals<br>• Value<br>• Judgments | Value judgments: reports on staff, estimates of the relative difficulties of jobs. (Stamper, 1973)<br>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?<br>Do the IS users feel that the current level of security is acceptable?<br>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?<br>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<br>• Instructions<br>• Plans<br>• Policies<br>• Orders | An order, a rule or a recommendation that will denote the objects to which the prescribed action must be related. (Stamper, 1973)<br>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?<br>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 of technical security?<br>Are IS users aware of the specific security policies in terms of the social aspects of security? |
| Affective Prescriptives<br>• Inducements<br>• Coercion<br>• Threats<br>• 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?<br>How much of a burden is security policy enforcement? | Have any personnel that have broken security policy actually been punished?<br>If they have been punished, are any of them repeat-offenders? |

**Table 2.1: Conceptual Framework for Semantic Analysis**

| **Power Element** | **Clegg's (2002) Description** | **Power Issues** |
|---|---|---|
| Episodic<br>• social relations<br>• agencies<br>• standing conditions<br>• outcomes | Episodes of day to day interaction, work, and outcomes whether positive or negative. | • What are the characteristics of the day to day social interactions between "managers" and "subordinates?"<br>• Does resistance impact the bottom line of getting things done at the organization?<br>• Is there an awareness of a sentiment of resistance in the organization?<br>• Has any direct impact come out of resistance in the organization?<br>• What are managerial reactions to subtle forms of resistance? |
| Dispositional<br>• rules fixing relations of meaning and membership | Socially constructed rules, membership categories (us/them), and mental maps or blueprints. | • Are there explicit power structures at the organization?<br>• Does the power behind explicit or implicit power structures get utilized when resistance arises? |
| Facilitative<br>• Innovation in techniques of discipline and production | Systems of rewards and punishment (disciplinary mechanisms) and the materiality of technology, job design, and networks. | • How is resistance dealt with at the organizational level when it becomes visible?<br>• Are there specific or sporadic consequences to resistance?<br>• If there are implied or specific consequences for resistance, are they enforced? |
| Meta-Circuit Influences<br>• Obligatory Passage Points<br>• exogenous environmental contingencies | Provides passage points empowerment and disempowerment. | • Are there any central points (human or procedural) that allow for members of an organization to circumvent power structures?<br>• If such points exist, how have members performed acts of resistance through such channels? |

**Table 4.1: Conceptual Framework of Power**

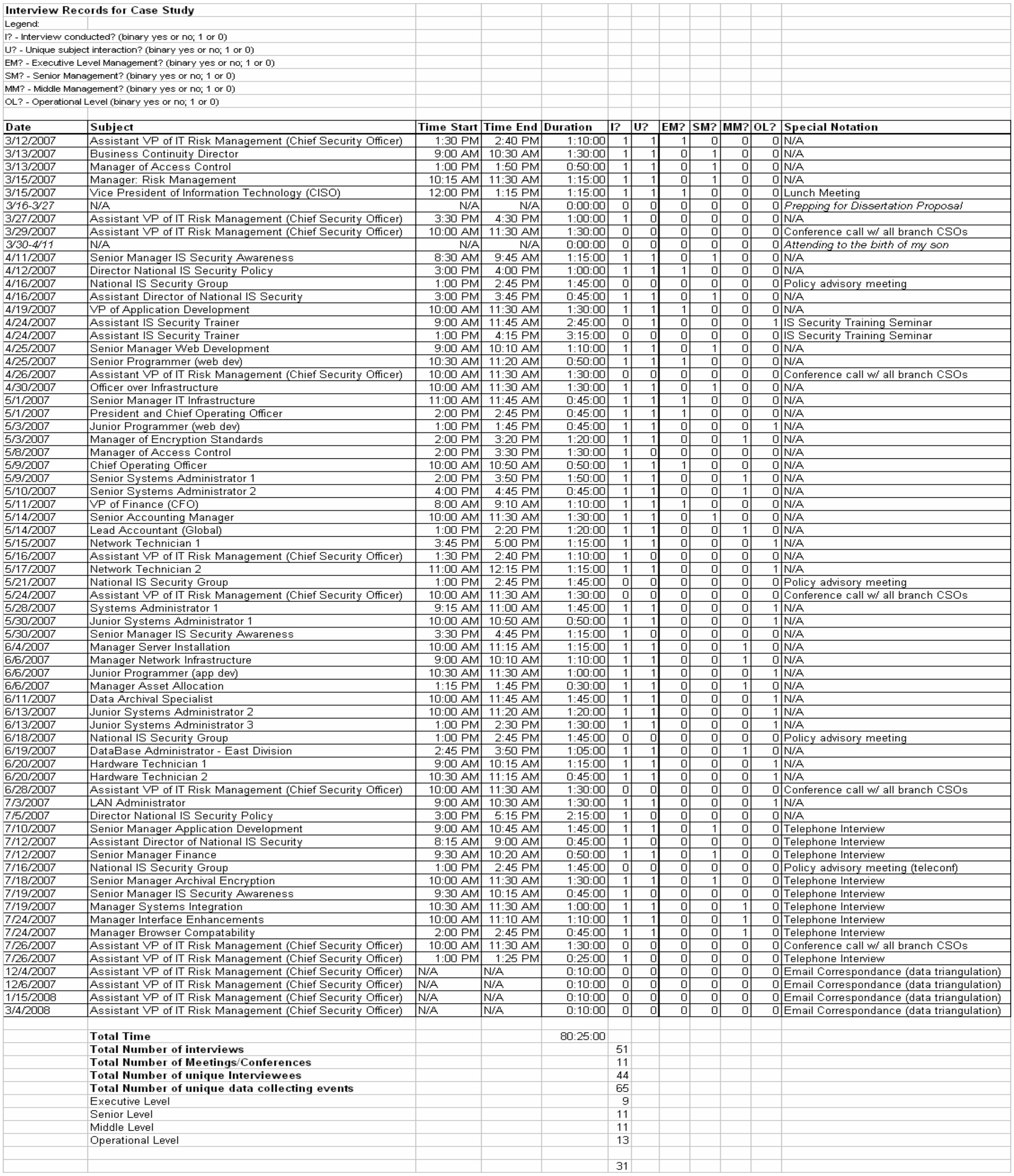


| | | Analysis on Productivity Performed Prior to IS Security Policy Implementation | |
|---|---|---|---|
| | | Yes | No |
| IS Security Policy Implementation Phased in? | Yes | IS Security Policy Implementation is Most Likely to succeed | IS Security Policy Implementation has Moderate Chance of Success |
| | No | IS Security Policy Implementation has Moderate Chance of Success | IS Security Policy Implementation is Least Likely to succeed |

*Table 7.1: 2x2 Table Illustrating the Practical Application of Findings*

# Appendix D

## Interview Records & Schedule



**Interview Records for Case Study**

Legend:

I? - Interview conducted? (binary yes or no; 1 or 0)

U? - Unique subject interaction? (binary yes or no; 1 or 0)

EM? - Executive Level Management? (binary yes or no; 1 or 0)

SM? - Senior Management? (binary yes or no; 1 or 0)

MM? - Middle Management? (binary yes or no; 1 or 0)

OL? - Operational Level (binary yes or no; 1 or 0)

| Date | Subject | Time Start | Time End | Duration | I? | U? | EM? | SM? | MM? | OL? | Special Notation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 3/12/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 1:30 PM | 2:40 PM | 1:10:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 3/13/2007 | Business Continuity Director | 9:00 AM | 10:30 AM | 1:30:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 3/13/2007 | Manager of Access Control | 1:00 PM | 1:50 PM | 0:50:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 3/15/2007 | Manager: Risk Management | 10:15 AM | 11:30 AM | 1:15:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 3/15/2007 | Vice President of Information Technology (CISO) | 12:00 PM | 1:15 PM | 1:15:00 | 1 | 1 | 1 | 0 | 0 | 0 | Lunch Meeting |
| *3/16-3/27* | N/A | N/A | N/A | 0:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | *Prepping for Dissertation Proposal* |
| 3/27/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 3:30 PM | 4:30 PM | 1:00:00 | 1 | 0 | 0 | 0 | 0 | 0 | N/A |
| 3/29/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 10:00 AM | 11:30 AM | 1:30:00 | 0 | 0 | 0 | 0 | 0 | 0 | Conference call w/ all branch CSOs |
| *3/30-4/11* | N/A | N/A | N/A | 0:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | *Attending to the birth of my son* |
| 4/11/2007 | Senior Manager IS Security Awareness | 8:30 AM | 9:45 AM | 1:15:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 4/12/2007 | Director National IS Security Policy | 3:00 PM | 4:00 PM | 1:00:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 4/16/2007 | National IS Security Group | 1:00 PM | 2:45 PM | 1:45:00 | 0 | 0 | 0 | 0 | 0 | 0 | Policy advisory meeting |
| 4/16/2007 | Assistant Director of National IS Security | 3:00 PM | 3:45 PM | 0:45:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 4/19/2007 | VP of Application Development | 10:00 AM | 11:30 AM | 1:30:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 4/24/2007 | Assistant IS Security Trainer | 9:00 AM | 11:45 AM | 2:45:00 | 0 | 1 | 0 | 0 | 0 | 1 | IS Security Training Seminar |
| 4/24/2007 | Assistant IS Security Trainer | 1:00 PM | 4:15 PM | 3:15:00 | 0 | 0 | 0 | 0 | 0 | 0 | IS Security Training Seminar |
| 4/25/2007 | Senior Manager Web Development | 9:00 AM | 10:10 AM | 1:10:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 4/25/2007 | Senior Programmer (web dev) | 10:30 AM | 11:20 AM | 0:50:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 4/26/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 10:00 AM | 11:30 AM | 1:30:00 | 0 | 0 | 0 | 0 | 0 | 0 | Conference call w/ all branch CSOs |
| 4/30/2007 | Officer over Infrastructure | 10:00 AM | 11:30 AM | 1:30:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 5/1/2007 | Senior Manager IT Infrastructure | 11:00 AM | 11:45 AM | 0:45:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 5/1/2007 | President and Chief Operating Officer | 2:00 PM | 2:45 PM | 0:45:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 5/3/2007 | Junior Programmer (web dev) | 1:00 PM | 1:45 PM | 0:45:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 5/3/2007 | Manager of Encryption Standards | 2:00 PM | 3:20 PM | 1:20:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 5/8/2007 | Manager of Access Control | 2:00 PM | 3:30 PM | 1:30:00 | 1 | 0 | 0 | 0 | 0 | 0 | N/A |
| 5/9/2007 | Chief Operating Officer | 10:00 AM | 10:50 AM | 0:50:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 5/9/2007 | Senior Systems Administrator 1 | 2:00 PM | 3:50 PM | 1:50:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 5/10/2007 | Senior Systems Administrator 2 | 4:00 PM | 4:45 PM | 0:45:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 5/11/2007 | VP of Finance (CFO) | 8:00 AM | 9:10 AM | 1:10:00 | 1 | 1 | 1 | 0 | 0 | 0 | N/A |
| 5/14/2007 | Senior Accounting Manager | 10:00 AM | 11:30 AM | 1:30:00 | 1 | 1 | 0 | 1 | 0 | 0 | N/A |
| 5/14/2007 | Lead Accountant (Global) | 1:00 PM | 2:20 PM | 1:20:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 5/15/2007 | Network Technician 1 | 3:45 PM | 5:00 PM | 1:15:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 5/16/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 1:30 PM | 2:40 PM | 1:10:00 | 1 | 0 | 0 | 0 | 0 | 0 | N/A |
| 5/17/2007 | Network Technician 2 | 11:00 AM | 12:15 PM | 1:15:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 5/21/2007 | National IS Security Group | 1:00 PM | 2:45 PM | 1:45:00 | 0 | 0 | 0 | 0 | 0 | 0 | Policy advisory meeting |
| 5/24/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 10:00 AM | 11:30 AM | 1:30:00 | 0 | 0 | 0 | 0 | 0 | 0 | Conference call w/ all branch CSOs |
| 5/28/2007 | Systems Administrator 1 | 9:15 AM | 11:00 AM | 1:45:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 5/30/2007 | Junior Systems Administrator 1 | 10:00 AM | 10:50 AM | 0:50:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 5/30/2007 | Senior Manager IS Security Awareness | 3:30 PM | 4:45 PM | 1:15:00 | 1 | 0 | 0 | 0 | 0 | 0 | N/A |
| 6/4/2007 | Manager Server Installation | 10:00 AM | 11:15 AM | 1:15:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 6/6/2007 | Manager Network Infrastructure | 9:00 AM | 10:10 AM | 1:10:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 6/6/2007 | Junior Programmer (app dev) | 10:30 AM | 11:30 AM | 1:00:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 6/6/2007 | Manager Asset Allocation | 1:15 PM | 1:45 PM | 0:30:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 6/11/2007 | Data Archival Specialist | 10:00 AM | 11:45 AM | 1:45:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 6/13/2007 | Junior Systems Administrator 2 | 10:00 AM | 11:20 AM | 1:20:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 6/13/2007 | Junior Systems Administrator 3 | 1:00 PM | 2:30 PM | 1:30:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 6/18/2007 | National IS Security Group | 1:00 PM | 2:45 PM | 1:45:00 | 0 | 0 | 0 | 0 | 0 | 0 | Policy advisory meeting |
| 6/19/2007 | DataBase Administrator - East Division | 2:45 PM | 3:50 PM | 1:05:00 | 1 | 1 | 0 | 0 | 1 | 0 | N/A |
| 6/20/2007 | Hardware Technician 1 | 9:00 AM | 10:15 AM | 1:15:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 6/20/2007 | Hardware Technician 2 | 10:30 AM | 11:15 AM | 0:45:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 6/28/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 10:00 AM | 11:30 AM | 1:30:00 | 0 | 0 | 0 | 0 | 0 | 0 | Conference call w/ all branch CSOs |
| 7/3/2007 | LAN Administrator | 9:00 AM | 10:30 AM | 1:30:00 | 1 | 1 | 0 | 0 | 0 | 1 | N/A |
| 7/5/2007 | Director National IS Security Policy | 3:00 PM | 5:15 PM | 2:15:00 | 1 | 0 | 0 | 0 | 0 | 0 | N/A |
| 7/10/2007 | Senior Manager Application Development | 9:00 AM | 10:45 AM | 1:45:00 | 1 | 1 | 0 | 1 | 0 | 0 | Telephone Interview |
| 7/12/2007 | Assistant Director of National IS Security | 8:15 AM | 9:00 AM | 0:45:00 | 1 | 0 | 0 | 0 | 0 | 0 | Telephone Interview |
| 7/12/2007 | Senior Manager Finance | 9:30 AM | 10:20 AM | 0:50:00 | 1 | 1 | 0 | 1 | 0 | 0 | Telephone Interview |
| 7/16/2007 | National IS Security Group | 1:00 PM | 2:45 PM | 1:45:00 | 0 | 0 | 0 | 0 | 0 | 0 | Policy advisory meeting (teleconf) |
| 7/18/2007 | Senior Manager Archival Encryption | 10:00 AM | 11:30 AM | 1:30:00 | 1 | 1 | 0 | 1 | 0 | 0 | Telephone Interview |
| 7/19/2007 | Senior Manager IS Security Awareness | 9:30 AM | 10:15 AM | 0:45:00 | 1 | 0 | 0 | 0 | 0 | 0 | Telephone Interview |
| 7/19/2007 | Manager Systems Integration | 10:30 AM | 11:30 AM | 1:00:00 | 1 | 1 | 0 | 0 | 1 | 0 | Telephone Interview |
| 7/24/2007 | Manager Interface Enhancements | 10:00 AM | 11:10 AM | 1:10:00 | 1 | 1 | 0 | 0 | 1 | 0 | Telephone Interview |
| 7/24/2007 | Manager Browser Compatability | 2:00 PM | 2:45 PM | 0:45:00 | 1 | 1 | 0 | 0 | 1 | 0 | Telephone Interview |
| 7/26/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 10:00 AM | 11:30 AM | 1:30:00 | 0 | 0 | 0 | 0 | 0 | 0 | Conference call w/ all branch CSOs |
| 7/26/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | 1:00 PM | 1:25 PM | 0:25:00 | 1 | 0 | 0 | 0 | 0 | 0 | Telephone Interview |
| 12/4/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | N/A | N/A | 0:10:00 | 0 | 0 | 0 | 0 | 0 | 0 | Email Correspondance (data triangulation) |
| 12/6/2007 | Assistant VP of IT Risk Management (Chief Security Officer) | N/A | N/A | 0:10:00 | 0 | 0 | 0 | 0 | 0 | 0 | Email Correspondance (data triangulation) |
| 1/15/2008 | Assistant VP of IT Risk Management (Chief Security Officer) | N/A | N/A | 0:10:00 | 0 | 0 | 0 | 0 | 0 | 0 | Email Correspondance (data triangulation) |
| 3/4/2008 | Assistant VP of IT Risk Management (Chief Security Officer) | N/A | N/A | 0:10:00 | 0 | 0 | 0 | 0 | 0 | 0 | Email Correspondance (data triangulation) |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **Total Time** |  |  | 80:25:00 |  |  |  |  |  |  |  |
|  | **Total Number of interviews** |  |  |  | 51 |  |  |  |  |  |  |
|  | **Total Number of Meetings/Conferences** |  |  |  | 11 |  |  |  |  |  |  |
|  | **Total Number of unique Interviewees** |  |  |  | 44 |  |  |  |  |  |  |
|  | **Total Number of unique data collecting events** |  |  |  | 65 |  |  |  |  |  |  |
|  | Executive Level |  |  |  | 9 |  |  |  |  |  |  |
|  | Senior Level |  |  |  | 11 |  |  |  |  |  |  |
|  | Middle Level |  |  |  | 11 |  |  |  |  |  |  |
|  | Operational Level |  |  |  | 13 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 31 |  |  |  |  |  |  |

# Appendix E

## Data Reduction and Analysis

| Episodic (Agentic) Power | |
|---|---|
| Interview Question & Exemplar Answers | Findings? |
| • Question 3 (What are the characteristics of the day to day social interactions between you and your superiors?)<br>• Subjects (EM)<br>o Interacts with his supervisor daily<br>o Disagreements → we come to a reasonable conclusion<br>▪ Pandemic was subject’s call (generic)<br>▪ Record Keeping was subject’s supervisor’s call (specific)<br>o “The Audit Dance”<br>▪ Auditors report to Board of Governors<br>▪ So they work internal but report external<br>▪ Report and discuss<br>▪ We come to a fair conclusion<br>▪ What actions do we take<br>o We’re all working towards the same mission<br>• Subjects (EM)<br>o “We agree to disagree”<br>o I have incredible respect for my boss… he’s very politically skilled<br>o 9/11 changed the Fed drastically<br>o Bus-Cont is the double red-headed step-child now… we had to start from scratch<br>o National perspective:<br>▪ IS Sec and BC policy are blending… it’s an organic process<br>• Subjects (SM)<br>o I’m an ‘E’ but my boss is an ‘I’<br>o We’re mutually encouraging to each other to ensure accurate feedback<br>o I have felt everyone out<br>• Subjects (EM, SM)<br>o The mgt style is laissez faire<br>o I do my own thing<br>• Subjects (EM, SM)<br>o We talk a lot… very collegial<br>• Subjects (MM)<br>o I have half a dozen bosses<br>▪ It’s take a degree of adjustment<br>▪ The “supervisor” role really goes away at the higher level<br>▪ I work through a VP at another organization<br>▪ I go around the normal chain of command<br>o System (national) Level: subcommittee of about 30 people…. It’s the classic herding cats problem<br>o You need to get a couple of balanced key thinkers… getting the right people will help get the whole group along<br>• Subjects (OL)<br>o There isn’t much in the way of discussion regarding problems<br>o Boss is nice but distant | o At a high level, very collegial and laid back, immense levels of respect… mutually encouraging to each other…. Laissez faire… people “do their own thing”<br>o Personality conflicts<br>o This came up a lot… a lot of reference to Myer’s Briggs<br>o Middle level, there is an issue of multiple reporting (half a dozen bosses)<br>o At the lowest, non-managerial level, there was a similar level of respect but the congeniality and laissez faire management style was absent. The rules and duties were clearly defined and the relationship was more professional.<br>o The most ambiguous (and thus most contentious) of the relationships was the local to national relationships as well as the branch-to-branch relationships<br>o 3rd party reporting (audit dance) |
| • Question 4 (What are the characteristics of the day to day social interactions between you and those that work for you?)<br>o Subject<br>▪ The closer you are to me (within the organization, relationship, or geographically), the less stringent the relationship is | o At the highest levels of the org, the laissez faire type relationship is very apparent.<br>o i.e. , if you have 2 managers at the same level, if one is physically closer in the office, he’ll have a |

| | |
|---|---|
| ▪ For example, if you have 2 managers at the same level, if one is physically closer in the office, he'll have a much looser relationship with them<br>o Subject<br>▪ 3 report to me (supervisors themselves)<br>• Great working relationship; professional & friendly<br>• Leadership → encourage discussion over disagreements<br>• Mutual respect<br>▪ There has however been resistance on a few occasions<br>• Person subversively resisted… he's gone now<br>o Subject<br>▪ Computer People don't want social interaction; they're very introverted<br>▪ Extroverted techies tend to be in the security side of IT/IS<br>o Subject<br>▪ Manager reports to me and is relatively new to I have to be hands on and carry her along<br>▪ Weekly team meetings<br>▪ Usually involved to small degree<br>▪ Interpersonally we are very collegial<br>• We collaborate on everything we do like the 3 musketeers<br>• Failure is taken personally<br>▪ Disagreements<br>• It's very open<br>• They're not susceptible to group think<br>• They may not bring it up right away<br>o Subject<br>▪ Casual relationship<br>▪ 100 developers… 10/10 meetings where I "skip level"… don't meet with managers but with workers<br>▪ Nothing I haven't known so far<br>▪ Resistance at first<br>o Subject<br>▪ I'm more detailed with managers<br>• It's really good<br>• Further down the hierarchy, the less collegial it is<br>o When we interact, it's project oriented<br>o When conflicts occur, we work it out<br>o When I'm adamant, they'll subjugate<br>o Subject<br>▪ Align ourselves with people we respect<br>▪ Conflict avoidance type of managers<br>▪ Collaboration and congeniality<br>• This has slowed down a lot<br>▪ Critical feedback<br>▪ Crucial confrontation/conversations<br>• Break down of expectations<br>• Someone breaks trust<br>▪ More people willing to speak up<br>▪ Myer's-Briggs used a lot | much looser relationship with them<br>o also still great working relationships that have mutual respect<br>o Disagreements… not susceptible to group think<br>o Upper level managers often skip a level and meet with lowest levels<br>o Sometimes sees resistance<br>o The further down the hierarchy, the less collegial it is<br>o The lowest levels do not have anyone working for them<br>o Try to avoid conflict<br>o Myers-Brigss used a lot<br>o More people willing to speak up (opposed to 15, 10, or even 5 years ago) |
| • Question 5 (Have you ever found fluctuations in your productivity due to intentional or unintentional resistance to security related management directives?}<br>o Subject<br>▪ Yes, I have found fluctuations in my productivity but I do not resist<br>o Subject<br>▪ It's not the wild frontier any more<br>▪ This has happened at the bank recently<br>▪ Rights have been taken away<br>▪ "Do I resist? Look at the plaque on my desk: *It's always easier to obtain forgiveness than permission*"<br>▪ You gotta know the people to fix things | o All of the subjects responded in the affirmative to this question and gave many examples of such<br>o They all gave various stories about how sec policy implementation has directly affected their job<br>o They also alluded to ways in which they have resisted the implementation |

| | |
|---|---|
| o Subject<br>▪ All the time<br>• Blackberry passwords<br>• Requirements changed out of the blue<br>• Very very annoying<br>• Nobody was asked<br>• FRIT (fed bank run out of NY branch)<br>o Subject<br>▪ ISAF 8 thing really slows things down… caused some turmoil<br>▪ Browser lockout – the developers have to have it<br>▪ Encryption takes time<br>▪ Plug ins take a while to get approved<br>▪ Getting around if was happening but that's slown down<br>▪ Things come down from system level<br>▪ She went to managers and manager<br>▪ Policy was tweaked out of necessity<br>▪ We suffered greatly until a compromise was figured out<br>▪ Hands are still tied<br>o Subject<br>▪ Absolutely<br>• "least user privilege" (no admin on your own pc)<br>▪ I give the sec officer a hard time all the time<br>▪ Help desk calls are through the roof<br>▪ Access to certain directories (i.e. HD for shared storage)<br>▪ Is it a major deal? NO… it's just annoying and it makes it take longer<br>▪ Inordinate amount of password resets… half of the help desk calls are PW related<br>o Subject<br>▪ Absolutely<br>▪ When I was chief sec. officer: "If you're doing your job, I'm not doing mine<br>▪ Examples<br>• Least user access<br>• HD encryption<br>• Not having access to data<br>• Insight into specific plans<br>o Looking for alignment<br>o The plans are on a need to know basis<br>▪ More clarification would be nice<br>▪ There is an encumbrance from a business continuity perspective<br>▪ I normally don't get annoyed… I keep up to date | |
| • Question 6 (Have you ever found fluctuations in your subordinate's productivity security related directives have been imposed?)<br>o Subject<br>▪ Policy that cannot be enforced is simply a recommendation<br>• i.e. token left in the USB port<br>• i.e. passwords on post-it notes<br>o Subject<br>▪ NO! – we are a very IS aware group… it used to be wide open though<br>o Subject<br>▪ There is usually grumbling and complaining but never actual resistance<br>▪ We're a very mature and secure organization especially since 2000 and on<br>▪ FRIT has been controlling things and that has been an area of contention<br>o Subject<br>o Groan and Moan but no actualized resistance | o In direct contrast to their own experiences, managers found that none of their subordinates had any impact on their job from security policy implementation |
| • Question 7 (To your knowledge, has a sentiment of resistance to new security measures ever been apparent in the organization?) | o This was split down the middle |

| | |
|---|---|
| o Subject<br>▪ I see a sentiment of resistance: ALWAYS<br>▪ INTJs<br>▪ We're all resistant to change as an organization but we collaborate<br>▪ Resistance was rarely, if ever, realized<br>• Blackberry issues were an example<br>o Policy came up for stronger passwords<br>o People went crazy<br>o We backed down and are now "taking a more reasonable approach" – easier password but HD is wiped if too many incorrect tries<br>o Subject<br>▪ Yes, there has been… examples:<br>• ISAF – no admin rights for PC<br>o Lots of complaining<br>o Hard to enforce this policy<br>o Subject<br>▪ I can't think of any<br>▪ We manage expectations before any implementation<br>▪ We do a marketing campaign<br>• Emails<br>• Messages in the monitors (strewn throughout the fed… elevators, hallways, etc)<br>• Office automation people in each dept that participate (trained ahead of time)<br>o Subject<br>▪ They think it's irritating but they know they need to do it<br>▪ Security is part of the culture<br>▪ They usually don't fight it<br>▪ Lots of audits: COSO audits<br>▪ Risk mgt processes<br>o Subject<br>▪ There's always resistance by management: "what's the benefit for me?"<br>▪ Blackberries | |
| • Question 8 (If there has been any kind of resistance to new security measures, has this resistance yielded any noticeable impact in the organization?)<br>o Subject: Not really<br>o Subject: Not really… no impact<br>o Subject<br>▪ Yes (audit helps in that regard)<br>▪ When people don't follow, they get spanked (explain, class, talk to manager, fired)<br>▪ A VP was trying to disable the autolock for the screen saver (he was bragging to the Senior VP in the elevator)<br>• I had to explain/inform and educate | o With few exceptions, everyone denied this<br>o There were a couple of interesting exceptions though |
| • Question 9 (Have you ever resisted (verbally or by action) any security measures imposed by the organization?)<br>o Subject<br>▪ Before I was the Chief Security Officer, we had a package to hold source… it was password protected…. I hacked into it a few times to get access (not malicious… only did it to get my job done quicker)<br>▪ I'd never do ^^^ now but I'm older now and I'm the security officer<br>o Subject<br>▪ Yes but it's not my nature to be subversive. I can find a way around it and I'll just go ahead and do it<br>▪ Social Engineering<br>• I am very trusted… if I ask for something, it'll | o This question was a more direct approach to resistance than question 5<br>o Again though, most people admitted that they do it |

| | |
|---|---|
| get done<br>• Your reputation ends up being a very big threat to an org's IS Sec… someone could theoretically abuse that<br>• Insider threat is critical: server admins an issue<br>o Subject<br>▪ I've tried to compromise on ridiculous security<br>• i.e. I'm looking to mitigate tape to get around the ridiculous tape encryption policy<br>• *this is a subversive action to get around the policy* | |
| | |
| Dispositional / Social Integration Power | |
| Interview Question & Exemplar Answers | Findings? |
| • Question 2: Who do you consider to be powerful within this organization?<br>o Subject<br>▪ Power of the Purse: Who has the funds?<br>▪ We all attempt to follow the spirit of the national policy<br>• i.e power-on password vs. HD encryption<br>• LAN patching<br>▪ There's a competing POV for what's the right thing to do<br>• "Not on my watch are you going to remove power on password<br>▪ The HW guys can do what they want… I wouldn't know but I have a good relationship with them<br>o Subject<br>▪ Senior VP is the most powerful: aligns with org structure<br>▪ Pandemic Planning – medical director<br>▪ US Treasury – external entity<br>o Subject<br>▪ We have power transfers via the treasury<br>• They control things… they are our customer<br>• It's always about the money and we have to satisfy them<br>▪ The power of knowledge<br>• Subject matter experts (Our techies)<br>o We depend on them and are a little subservient to them<br>o Not necessarily running the show but they will have a say<br>• Technology is power<br>o Subject<br>▪ Definitely an alignment with hierarchy BUT<br>▪ There are a number of subject matter experts… more "influencing" from the lower level<br>o Subject<br>▪ We have radical thinkers (ISTJs) in development that want to try things that aren't standard<br>▪ Technical knowledge – respect means a lot for a team leader<br>▪ There is an application architect<br>• He is isolated and is responsible for decisions<br>• Proposes new standards<br>o Subject<br>▪ The power structure changed with the nationalization & standardization (2000/2001) of the IT function<br>▪ He's now outside the local system influence<br>▪ He wanted to resist the nationalization of his job… it's been a hard adjustment for his staff<br>▪ We still worry about the rollout (implementation)<br>▪ Nationalization:<br>• Due to cost savings (80%)<br>• Increased security<br>• Makes sense to centralize<br>▪ "The power of the server admin" – I'm aware of what they | o The people who have control over the money have the real power<br>o The people who have technical knowledge have the real power<br>o "The Power of the Server Admin"<br>o They have a great degree of power<br>o Subject matter experts<br>o The HW guys do what they want<br>o Technical Knowledge<br>o There are external entities that really pull the strings<br>o The power structure changed with the nationalization/ standardization of IT<br>o The people that have the explicit power (organizationally) also have the real power |

| | |
|---|---|
| can do… they have a great degree of power<br>o Subject<br>▪ The org is maternalistic… people are happy within their roles | |
| • Question 10: What are you thoughts on the explicit organizational structures (from mid-level management to executive management) at this organization?<br>o Subject<br>▪ The trusted role can override the org structure<br>• I have a circle of control and a circle of influence<br>• I am very trusted… if I ask for something, it'll get done<br>• Your reputation ends up being a big threat to an org's IS Sec<br>• Someone could theoretically abuse that<br>▪ In the heat of the battle, if there is a threat/risk, you don't ask questions or argue<br>o Subject<br>▪ The explicit structure is NOT well known nor understood, especially taking the system/national perspective into account<br>▪ The IT function appears well defined but it isn't clear<br>• Who decides what changes are made?<br>• Herding cats again<br>• The path of a decision has a lot of variance<br>o It used to be clear cut at the local level but the scope of the policy makes it less and less clear<br>o Hybrid mix of local and national IT<br>o Sometimes the path gets invented – i.e. I made my own procedure for approving | o The structures are not well known nor understood<br>o Especially taking the movement towards nationalization<br>o The path of a decision has a lot of variance<br>o Sometimes the path gets invented<br>o The trusted role can override the org structure |
| • Question 11: In the instances when resistance to security measures has come about, what kind of reaction has there been from those supervisors in the organization?<br>o Subject<br>▪ We have violation reports<br>• I'll go the manager and tell them then the mgr goes the employee<br>• It's good to work the politics<br>• We've got a person that follows up on violation reports<br>• It's all documented<br>• Can result in "targeted" awareness training<br>• People do some stupid stuff… everything is monitored… people go to bad sites: instant firing<br>o Subject<br>▪ Responsibility statements<br>▪ Re-do security training | o Violation reports<br>o 3rd party follows up with these<br>o Some conflict as to the degree of punishment<br>o Some upper level deny it's gone further than additional awareness training<br>o Others know of people that have been fired for certain things |
| • Question 17: Has your immediate superior ever given you the go ahead to ignore particular security measures in order to avoid "making your job harder than it needs to be?"<br>o Subject:<br>▪ When I was a young programmer and was stuck, my boss told me to just ignore the security and hack in<br>o Subject:<br>▪ (laughs), NO, never!<br>▪ My old job was awful though, security was a window dressing<br>o Subject:<br>▪ Previous ISO to me: Support a test for a financial organization<br>▪ Encrypted communications between mainframes<br>▪ Parameter was set incorrectly | o in the past some had but always in line with the mission of the company… never malicious |

| | |
|---|---|
| • He didn't have access rights<br>• ISO couldn't help me (she was not technically astute)<br>• Question 18: If questions 14 or 15 are "yes," how have you followed through with it?<br>o Subject 7<br>o He asked permission to breach security and he got it | |
| | |
| Facilitative (System Integration) Power | |
| Interview Question & Exemplar Answers | Findings? |
| • Question 12: In the instances when resistance to security measures has come about, have you noticed any informal compromises and agreements come about that directly deal with the security issue?<br>o Subject<br>▪ Passwords used to not be automated<br>▪ PWs were being cracked to monitor compliance<br>▪ Now that they're automated, the cracking percentage has dropped from 30% to near 0%<br>o Subject<br>▪ Firefox issue – we fought back<br>▪ FISMA testing<br>▪ 9/11 shift was apparent<br>▪ security practices are getting productivity related<br>▪ the education process is critical – it really helps a lot<br>• Question 13: Has resistance to security measures been discussed at an organizational level (i.e. via security awareness programs)? If so, what was your reaction to this discussion?<br>o Subject<br>▪ They're looking for an explanation<br>• They know it's important<br>• You know you're going to get confrontations from time to time<br>▪ "security's evolved into something that's mainstream"<br>• therefore not as many confrontations<br>▪ I took part in security awareness and was told I'd be fired if I did not comply<br>▪ We do personality checks/screening for server admins<br>• Question 14: Are you aware of any specific consequences to resistance to new security measures by employees?<br>o Subject<br>▪ There's a fair amount of latitude<br>▪ There are rules that people have to abide by<br>▪ No one has been fired<br>▪ We run cracking tools monthly looking for weak passwords<br>• Series of increasing steps if they just can't get it right<br>• They may end up in remedial class which is embarrassing (shaming?)<br>• One employee used obscenities in his password to send a msg to the security people<br>▪ A few people have not wanted to comply<br>• A guy was ugly in email replies<br>• Pornographic, gambling, hate sites are currently blocked… people have been fired though<br>• Question 15: If there are implicit or explicit consequences for resistance, are they enforced?<br>o Subject<br>▪ Pretty well enforced here<br>▪ Bank has a very ethics level.. hard to sugar<br>▪ Senior leadership are very serious about security<br>• Question 16: If you are given a new security directive that might negatively impact your productivity, have you ever found a way around the new security directive? | o Two major areas in system integration: production & discipline<br>o Production: standardized and sanitized<br>o Discipline: on the surface, it is the same as production but deep down there are variances |

# Vita

Michael Stephen Lapke was born on May 6th, 1975 in Weston-Super-Mare on the west coast of the United Kingdom. Born of Irish parents, he held both British and Irish citizenry upon birth. He immigrated to the United States in 1980 with his mother and upon adoption by his stepfather, became a US citizen in 1982. He graduated from Mountlake Terrace High School in Seattle, Washington in 1993. He received his Bachelor of Science in Computer and Information Science from the University of North Florida in 1999 and subsequently worked at Alltel Information Systems as a COBOL programmer for one year. He soon returned to school and received a Master of Science in Computer and Information Systems from the University of North Florida in 2001. During the course of his Master's degree he was awarded a teaching assistantship which covered his tuition and paid a stipend. Upon graduation, he was offered a position as an instructor at UNF.

During the two years of full time employment at UNF, Michael taught a wide variety of computer science and information systems courses. These included Introduction to Java, C, and COBOL, as well as File Structures, Computer Hardware, Systems Analysis and Design, Systems Implementation, and graduate courses in Database Design and Information Systems Security. During his tenure at UNF, it became apparent that a doctorate degree would be necessary to continue in the academic field.

Michael was accepted to Virginia Commonwealth University's PhD in Information Systems program in 2003. He plans to graduate in the spring of 2008 with his degree in hand. Between the 2004 and 2007 years of residence at VCU, Michael was awarded a graduate assistantship that covered his tuition costs. He was also employed by the Information Systems Department as an Adjunct Instructor. As an Instructor with VCU, Michael taught Introduction to Java, Database, Network Applications, and Introduction to Information Systems.

During the three year span between 2004 and 2007, Michael also formed his own company, Lapke Consulting, LLC. As president of the company, Michael worked with regional companies such as First National Brokerage Corporation and Ameronix Corporation as a freelance database and web developer. Michael led these companies towards bringing several large networked systems online. Michael disbanded the company in 2007 when he was offered a professorship in Florida.

Since 2007, Michael has been employed as an Assistant Professor at Florida Institute of Technology. In his position at FIT, he has led the development of a new bachelor's program in Computer Information Science. As the Program Chair of this new program, he has created the curriculum and class content for the entire degree. He currently employs adjuncts to fill the need for instructors and manages approximately 20 employees including administrative personnel and adjunct instructors. Besides these duties, he also teaches in the graduate and undergraduate CIS programs.