2008

Power Relationships in Information Systems Security Policy Formulation and Implementation

M Lapke
Virginia Commonwealth University, lapkems@vcu.edu

Gaurpreet Dhillon
Virginia Commonwealth University, gdhillon@vcu.edu

POWER RELATIONSHIPS IN INFORMATION SYSTEMS SECURITY POLICY FORMULATION AND IMPLEMENTATION

Lapke, Michael, Virginia Commonwealth University, 301 W. Main Street, Box 844000, Richmond, VA 23284-4000, lapkems@vcu.edu

Dhillon, Gurpreet, Virginia Commonwealth University, 301 W. Main Street, Box 844000, Richmond, VA 23284-4000, gdhillon@vcu.edu

Abstract

This research argues that organizational power impacts the development and implementation of Information Systems (IS) Security policy. The study was conducted via an in depth case study at the IT department within a large financial organization in the United States. The theoretical foundation for the research was based was Clegg's (2002) Circuits of Power. A conceptual framework was created utilizing Circuits of Power. This was used to study power relationships and how they might affect the formulation and implementation of IS Security policy in this organization. The case study demonstrated that power relationships have a clear impact on the IS security policy process. 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.

1. THE NATURE AND SIGNIFICANCE OF POWER RELATIONSHIPS AND IS SECURITY POLICY

IS Security policy is of core importance to an organization's overall IS Security (Hone & Eloff, 2002; Warman, 1992). This is a result of a 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 & Solms, 2004a). Without this anchoring point, security projects and efforts "will be floundering around without really making progress" (Solms & Solms, 2004a, p. 374).

Despite the agreement of the criticality of IS security policy, little research has explored how good security policies are created (Baskerville & Siponen, 2002).While there is not much empirical research that addresses the result of non-compliance to IS Security policy (Doherty & Fulford, 2005), the logical inference is that non-compliance would lead to the security of an organization being questionable (Solms & Solms, 2004a). While not directly addressing the question of the extent to which a security policy affects overall security effectiveness, research has shown its presence is important in reducing security breaches (David, 2002; Loch et al., 1992; Solms & Solms, 2004a; Whitman et al., 2001).

We argue that organizations fall short of achieving the most effective formulation and implementation of IS Security policy by overlooking power relations. The 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 paper is organized into five sections. Following a brief introduction, the nature and significance of power relationships is reviewed and a framework for analyzing power is introduced. The framework is then used to interpret power

relationships in the case study. After a discussion on various power relationships prevalent in the case study, conclusions of this paper are presented.

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.

The literature is lacking in the way of power relationships and IS Security Policy but the relationship between power and information systems has been extensively studied. Our intention is not to present a detailed review of literature; rather the objective is to touch upon some of the key concepts from the extant literature. Markus and Bjorn-Andersen (1987) explored how information systems professionals were exercising power on users, using Lukes' conception of power. This is instantiated when entity A exercises power over entity B, despite B's own interests (Lukes, 1974). Lukes' concept of power was challenged by Clegg (2002) and Law (1991) in two fundamental ways. First, the idea of interests introduces moral relativism because the researcher, in order to identify the exercise of power should attribute interests. Second, Lukes' concept neglects the idea that power is a relationship thus reducing it to a capacity. The insights derived from this work are that power exercise not only involves computers and information systems but also the selection of appropriate methods and policy formulation.

Security policy could be approached in the same manner as Walsham (1993), who suggests a framework, for interpreting information systems. Information systems, Walsham claims, are power instruments because they have embedded rules. However, the relationship between IT and power is not spelled out in this framework. What is needed is an analytical framework that helps us to interpret the nature and significance of the embedded rules within the formulation and implementation of IS security policy. In this paper we have applied Clegg's (2002) Theory, Circuits of Power. The following section describes briefly our framework, which integrates most of the insights of previous research. The most important contribution of the framework is the focus on how power relations affect the formulation and implementation of IS Security Policy.

2. AN INTEGRAL FRAMEWORK FOR ANALYZING POWER

Clegg's (2002) circuits of power model (see figure 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.

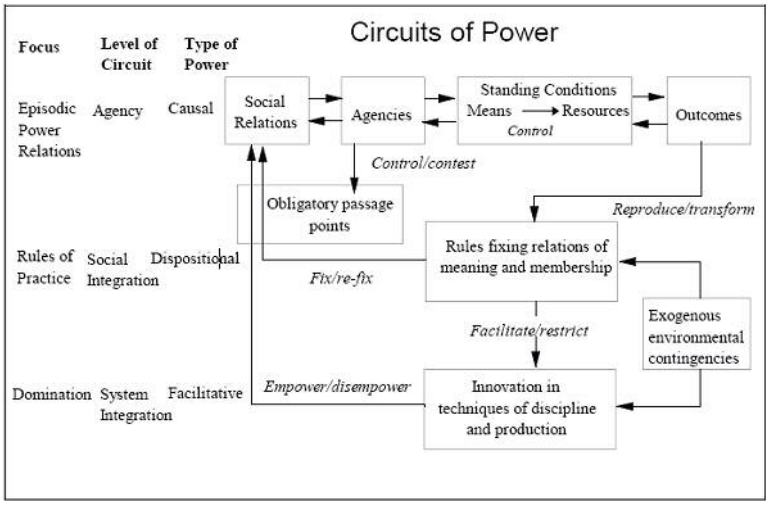

Figure 1. Circuits of power (Clegg, 2002)

2.1 The episodic circuit of 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, p. 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.

2.2 The circuit of social integration

The circuit of social integration was 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, p. 224). It has also been 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, social integration looks more at how social structures impact power relationships. With this perspective, the research focused on two particular subunits within this level of Clegg's circuits of power: membership and shared norms. Membership refers to organizationally defined or implicit group structures within the organization. The second subunit, shared norms, can also be described by cultural characteristics (Silva, 1997).

One of the reasons why an organization may have ineffective IS security is the lack of fit between the new meanings arising from the implementation of IS Security Policy and the prevailing organizational rules and norms. In any organization, tension will arise as a consequence of the 'lack of fit' between the institutional order and its material condition. The material condition is constituted by technology, techniques and methods of production, whereas the core institutional order will be integrated by the

values, beliefs and norms already institutionalized in the organization. The lack of fit will be characterized by a type of 'strain' stemming from the incompatibility between the institutional order and the material base. In the case of this lack of fit, the material conditions, according to Lockwood (1964), will engender social relationships and practices that can threaten the organization. The consolidation of these social relationships and practices will depend on the success with which managers are able to cope with the disintegrating tendencies within the organization (Lockwood, 1964, p. 252). The circuit of social integration will comprise the norms, rules and meanings that identify and allow the integration of a particular group. The realization of this circuit will allow security personnel to incorporate in the implementation of IS security policy those characteristics that are essential for establishing a fit in the organization.

2.3 The circuit of system integration

System integration 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, 2004, p. 224). Besides the material means of production, System integration deals with facilitative power because the material conditions of production might empower or disempower agencies. Clegg stresses that the concepts of production and discipline cannot be separated. The circuit of system integration is the major source of change in the circuits of power framework, particularly when the material conditions of production are altered. System integration, as a result of new techniques of discipline and production, is a potent source of transformation and tension, hence its relevance to our field. It implies new agencies and new obligatory passage points that the circuit of social integration might find difficult to resolve (Clegg, 2002). That is why the implementation of IS security policy will always be contentious. Success in implementation will depend greatly on the managerial ability to translate the new rules and norms implied by the system into pieces of discourse that other members of the organization can understand and accept.

The circuit of system integration is fundamental to understanding power relationships in IS security policy formulation and implementation because it helps us to understand the way IS security policy can be shaped by power. To identify this circuit, analysts should focus on how information systems will be used as a means of control and discipline. It can be anticipated that those groups that will be under control by the system might resist. When examining IS security policy formulation and implementation through the lens of system integration, the researcher is seeking an understanding of informal compromises regarding resistance to security, procedures for dealing with resistance to security, consequences to resistance, and enforcement of those consequences.

3. THE CASE STUDY

The research was conducted via interpretive case study at the aforementioned financial organization over the span of six months between 2006 and 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, p. 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 was created from Clegg's (2002) Circuits of Power as described previously. The method involved data gathering primarily via semi-structured interviews guided by the theoretical framework. These interviews focused on the upper level management of the organization, particularly in the Information Systems and IS security executive level management. Of the 60 personnel interviewed, 70% (42) of the subjects were classified as upper level management within the organization. These included the president (CEO), Chief Operating Officer, 12 senior vice presidents (including the CIO, CISO, CFO, CFO, and CPO), 20 division officers, and eight 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. Most 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). 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.

3.1 Brief description of IS security policy at Millennium Bank

The case study presented in this paper concerns the shift towards a nationally based standard for IS security policy at Millennium Bank. IS Security at Millennium Bank is designed to protect information from loss or misuse, and thereby to minimize the risk of monetary or productivity loss as well as embarrassment to the bank. One component of the program is an IS 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. The assessments consider both the likelihood and impact of the threats.

Most nationwide information technology activities are consolidated under NLIT. 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.

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

3.2 Episodic Power within Millennium Bank

At the highest levels of the organization, the various relationships between subjects and their superiors appeared casual in nature. The upper level managers had considerable respect for their immediate supervisors. This respect was bi-directional as they were typically allowed to perform their duties via a laissez faire management style. The subjects were 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 felt 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."

Regarding the subject's perception of the general attitude towards IS Security Policy implementation, there was a mixed response. The highest levels of management mirrored the non-management employees. This is to say that both groups always perceived a sentiment of resistance to new security measures. With that being said, the highest levels of management felt that the organizational collaboration was smooth enough to offset any negative outcomes. On the other hand, instead of the positive picture painted by the executives, the non-management employees had 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 a fundamental part of life at Millennium Bank. To this group of subjects, it was illogical that there could be an air of resistance when security was 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 (Culbert & Mcdonough, 1980; Pfeffer, 1981; Porter et al., 1983). 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 were more pragmatic in their perspective. Their responsibilities did not limit themselves to employees; rather the entire organization was 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 moved towards a more concrete view of resistance. To do this, the researcher asked the subjects whether or not they had ever verbally or physically resisted IS Security Policy implementations. 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 (Ceraolo, 1996), subversive resistance (Collinson, 2002), and feigned ignorance (Mcdonough, 1971).

The most striking example of subversive resistance was described by the business continuity (BC) manager. The bank implemented a new security policy that required that all data tapes be encrypted. To avoid the cost of the encryption machines, the BC manager instead changed from tapes to disks to backup the data. He did this for the overt reason of avoiding the new security policy.

This manager was 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 was 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 investigate 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 throughout 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 was simply representative of management saving face. The exceptions to this rule were the employees who were directly involved in IS Security Administration. They knew that security was rarely a readily accepted reality in any organization and did not have many illusions about this fact.

3.3 Social and system integration within Millennium Bank

To better understand the context of the groups and membership within Millennium Bank, 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). 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 & Arief, 2004; R. Solms & Solms, 2004b) 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 at this organization. The first level, the security artifact, was abundant throughout the organization. Armed guards, locked and armored doorways, monitored hallways, and smartchip ID badges demonstrated physical security was critical. The second level, espoused security values, was evident throughout the organization. The site had 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 was not possible to move around the organization without being subject to constant reminders of the importance of security. Also every employee of the bank was 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 one 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 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, network hardware, and portable devices. A second subset of technologists 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 final outcome expected from the introduction of a national IS security policy standard within Millennium Bank was to improve the effectiveness of IS security throughout the entire bank structure. Standardizing the policy was anticipated to reduce redundancies and conflicting IS security policies throughout the various branches of the organization. Senior management in Millennium Bank considered the introduction of national standards as a means of achieving a consensus and cohesion of IS security within the organization. It was therefore felt that this would enable the organization to improve the effectiveness of IS security across the whole of the organization.

4. DISCUSSION

The mutually transformational relationship between IS Security Policy implementation, resistance, and productivity is an emergent theme that arose during the course of the research. It was 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 was 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. Baskerville (1993) and Siponen (2001) report that social implications of IS Security are at best afterthoughts. 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 & Arief, 2004).

Though not as strong a relationship as the effect of IS Security policy implementation on resistance, there still was evidence of the reverse end of that particular relationship. That is to say that the resistance had 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 & Arief, 2004; Schultz, 2004). With this piece of the puzzle in place, the mutually transformational relationships can be seen in Figure 2:

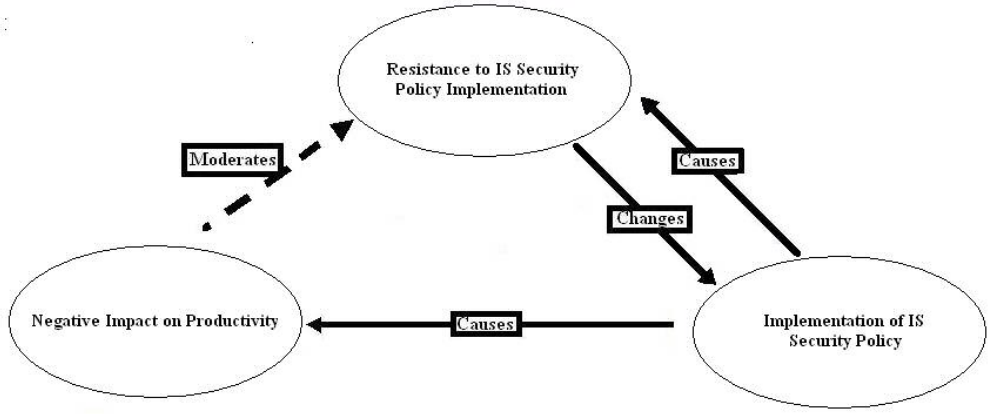

Figure 2: The mutually transformative relationship between IS security policy and resistance

Figure 2 demonstrates the mutually transformative relationship between the implementation of IS security policy and the resistance to that implementation. In other words, the implementation will cause 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. Thus, the greater the resistance, the more likely it will cause a change to the policy.

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 (Orlikowski, 1993; Peppard, 2007; Pettigrew, 1972; White & Leifer, 1986). 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 is the NLIT group and are 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 violate policy. It would be very difficult for their managers or security staff to become aware of this lack of compliance. 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.

The interaction between NLIT and IS Security executives was restricted to the highest levels of the organization. Since NLIT's initiatives were intended to be national, all of the CSOs in every branch were involved in the advisory effort. To coordinate this, they created an advisory committee which met regularly via teleconference. The intent of these meetings was to establish a consensus of advisory points for the NLIT towards formulating an IS Security Policy at a national level. The relationship between the three power broker groups and the IS security policy is displayed in figure 3:

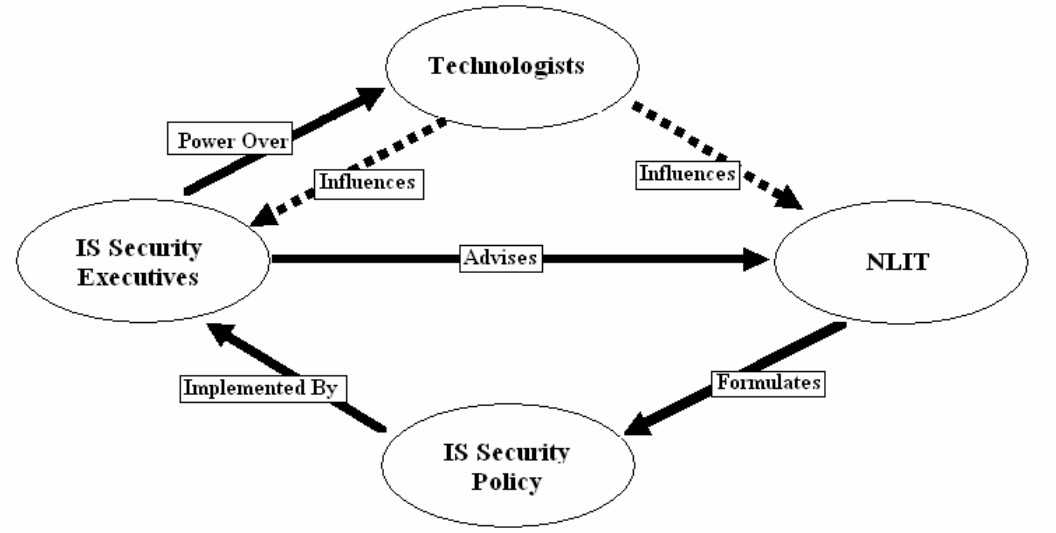

Figure 3: The power brokers impact on IS security policy

Figure 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 figure 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 literature and is a fruitful area for future research.

5. 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. Our analysis 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, we propose an analytical tool: The Circuits of Power Framework. We also interpret the nature of resistance and the effect of implicit power groups within the site. As expected, there was clear evidence of resistance to the implementation of IS security policy within the organization. The nature of the resistance was heavily influenced by the perceived impact on productivity however. As the effect the policy implementation had on productivity increased in scope, the resistance to the implementation increased 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 was 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 acknowledged, and to a degree expected, their input but it was 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 has demonstrated 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.

References

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

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

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

Bloomfield, B. P., & Best, A. (1992). Management consultants: systems development, power and the translation of problems. The Sociological Review, 40(3), 533-560.

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

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

Collinson, D. (2002). Managing Humour. Journal of Management Studies, 39(3), 269-288.

Culbert, S., & Mcdonough, J. (1980). The Invisible War: Pursuing Self-interests at Work, New York.

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

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

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

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

Law, J. (1991). Power, discretion and strategy. In J. Law (Ed.), A Sociology of Monsters: Essays on Power, Technology and Domination (pp. 165 191). London: Routledge.

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

Lockwood, D. (1964). Social Integration and System Integration. In G. K. Zollschan & W. Hirsch (Eds.), Explorations in Social Change (pp. 244 257). London: Routledge & Kegan Paul.

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

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

Mcdonough, J. (1971). The Accountant, Data Collection and Social Exchange. The Accounting Review, 46(4), 676-685.

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

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.

Pfeffer, J. (1981). Power in Organizations. John Wiley, Chichester.

Porter, L., Allen, R., & Angle, R. (1983). The politics of upward influences in organizations. In R. Allen & L. Porter (Eds.), Organizational Influence Processes (pp. 408-422). Glenview, IL: Scott Foresman.

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

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.

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

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

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

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

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

Warman, A. (1992). Organizational computer security policy: the reality. European Journal of Information Systems, 1(5), 305-310.

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

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

Willison, R. (2002). Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank. Unpublished Dissertation, London School of Economics, London.