

Organizational Power and Information Security Implementation

Jon Blue¹ and Gurpreet Dhillon²

¹University of Delaware

²Virginia Commonwealth University

Abstract—This purpose of this paper is to show how the implementation of information systems security policies in an organization can be improved by applying a power exercise model. It argues that stakeholders' awareness of the power being exercised by the policy enforcers, affects the success of the policy implementation. The model is developed by adapting, and extending, a power exercise framework presented by Markus and Bjørn-Andersen [20]. The information systems security policy model is applied to the introduction and compliance of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at HealthCo Systems, a non-profit health care organization in a major United States city.

Index Terms—Organizational Power, Power Exercise, IS Security Policy, Policy Implementation, Compliance, HIPAA

I. INTRODUCTION

THIS paper shows how the awareness of the power brokers in an organization can assist management in successfully implementing information systems security policies. There continues to be a high level of attention on the successful development and implementation of information systems security policies. While most organizations have developed a security policy, many have now turned their attention to successfully implementing these policies. In this context, success equates to employee compliance. Compliance has become a greater concern, not just because of potential threats to an organization's information, but also because over the past few years there has been an influx of regulatory and compliance mandates by the United States government. Some of these mandates, such as the Financial Modernization Act of 1999¹ (known as the Graham-Leach-Bliley Act), applies to all corporations. Others, such as the Health Insurance Portability and Accountability Act of 1996² (HIPAA), are applicable to certain industries [29]. Executives' concerns of compliance are warranted because employee non-compliance to information systems security policies can be fiscally devastating.

It is believed that the successful implementation of information systems security policies will increase with an

awareness and appreciation by all stakeholders of the use of power and politics in organizations. These stakeholders consist of employees, who are directed to follow policy, and management, who are responsible for enforcing compliance. Actually, management usually empowers their *agents* to act on their behalf to ensure employees adherence to organizational policies. It is imperative to view the failed implementations of security policies from a power perspective because power assists in realizing change [7] – which is needed when the institutionalization of security policy compliance is desired. It is unfortunate that power is still viewed as negative by many [19], as oppose to how power is presented in this paper – as a phenomenon to be aware of by all stakeholders in order to obtain the most beneficial result. In this case, the positive output is the successful implementation of information systems security policy, which is employee compliance.

While it may be equally important to look at the development of information systems security policy from a power perspective, the purpose of this study is to show how the implementation of information systems security policies can be improved. This work takes for granted that the security policy is in existence. Markus and Bjørn-Andersen [20] present a framework that specifically looks at the exercise of power by IS professionals over systems users. This paper adapts the Markus and Bjørn-Andersen framework in order to model the exercise of power by information systems security agents over employees and its impact on successful policy implementations.

II. LITERATURE REVIEW

A. Power and Information Systems

The term power is used quite interchangeably in the literature to represent differing conceptualizations of power: power, politics, authority, legitimacy [2][5][9][12][19][24][31]. Hall [14] capsulated power by stating that “power has to do with relationships between two or more actors in which the behavior of one is affected by the behavior of the other.”

Given these diverse definitions, there have been numerous attempts to define and measure the theoretical construct of “power” in organizations. Unfortunately, this has been done in different ways, which has led to varying results. One reason for this difficulty is that power not only has visible characteristics, but there are also many invisible characteristics [31]. Another reason for this difficulty is that many disciplines (e.g., management, sociology, marketing, political science) have been used as referenced disciplines to describe the interaction

¹ Includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

² Administered by the U.S. Department of Health and Human Services, a set of national standards for the use and disclosure of individuals' health information as well as standards for individuals' privacy rights to understand and control how their health information is used [23].

between power and information technology [17]– which has resulted in definitions that have been discipline specific and inconsistent.

Over many years, there have been multiple suggestions by researchers on how organizations can, and should be viewed, to explain and describe organizational phenomenon. Jasperson et al. [17] use four power lenses to view the role of power/organizational politics and different information technology outcomes. These views are rational, pluralist, interpretive, and radical. The Jasperson et al. lenses are projected from Bradshaw-Camball and Murray [6] who specifically use a trifocal lens of functionalist, interpretive and radical. Both views are adapted from Burrell and Morgan [8]. Rational power is defined as structural power which is focused on information, authority, and expertise as bases of power. This is where power is viewed as an objective reality. The pluralist lens of power assumes an objective definition where conflict is normal. In this view, the development, prioritization, and execution of goals are political and involve negotiation based on the control of information and resources. When power is based on the ability to control access to, and direct the construction of organizational realities, then the interpretive lens is being used. Similar to other interpretive views, power is socially constructed and the stakeholders exert influence by constructing the meanings of others. Lastly, the radical view looks at power and politics as the result of social structures (e.g., class, gender, institutional structures, race) that are exogenous to the organization. Bradshaw-Camball and Murray [6] say that political activity (broadly defined) involves either maintaining or undermining (and ultimately overthrowing) the current power structures [17].

An additional theory that describes power's use in organizational teams such as information systems is the "strategic contingencies theory" [16]. If a team is in a central part of the workflow of an organization, then what they do is very important. This gives them many opportunities to be noticed. It also means that they are on the critical path to success, such that if they are not involved, the whole show stops -- again creating attention and giving them bargaining power. Finally, if they are difficult to replace (e.g., because of their knowledge or skill level), then enemies that are made up of the hierarchy cannot just move the powerful team out, or sideways.

Organizations that are responsible for information systems security policy implementation and compliance are often housed in the information systems department. The strategic contingency theory suggests that these agents are in the teams that are quite powerful in organizations and have power that is described by the theory. As stated, Markus and Bjørn-Andersen [20] point out that testing has shown that other departments do not consider information systems departments as having power. However, Clegg [9] described a specific form of power as a set of capabilities and purported that having power does not mean you have to use it. This being said, it is quite possible that employees do not necessarily see power used by information systems professionals and therefore equate this to them not having said power.

... some social actors, who might be potentially powerful, may not recognize the [sources of power] or the fact that they possess them.... Even if power positions are recognized, organizational actors may choose not to employ their power [20].

While power is a very significant base in our proposed model, as important is information systems security policy.

B. Information Systems Security Policy

Information Systems security policy can be fractioned into the development, and implementation (rollout and enforcement). While there is wide standing agreement that a good information systems security policy begins an organization's information security, there is little work on the development [3], and implementation of good security policies.

As presented by Baskerville and Siponen [3], definitions of security policies, fall into two camps: non-technical/security management and technical/computer security. In defining the non-technical/security management, Wood [33] states that 'policies' are statements that come from high management and mid-level management enforce 'standards' that are more specific and often direct technological standards that conform to high level management policies. He reserves the term 'procedure' for the actual method of how the policies are implemented. Dhillon [11] differentiates strategy, policy, and operating procedures and purports that instead of developing policies, organizations should develop an information security vision and strategy at the apex of the organization.

In defining the technical/computer security, security policy is viewed by some, on one end of the continuum, to be from security architectures of operating systems [3][31]. Other researchers present security policy on the opposite end of the spectrum: controlling the access to systems by rules [26]. As presented by Sterne [30], a different perspective is presented that is between these two extremes and presents three security policies. These policies are objective (protects an identified resource from unauthorized use), organizational (description of how to achieve security policy objectives), and automated (how a computer systems protects computer resources according to an organization's security policy) [3]. Abrams and Bailey [1] offer an additional technical view. They distinguish three views of security policy: top management's view, users' view, and the designer's view.

C. Power and Information Systems Security Policy

Where there is literature present in each of the domains of power and of information systems security policy, as presented above, absent is literature that views these policies through a power lens. Given the different views of organizational power as stated earlier, there can be as many different ways to explain the failure of these implementation attempts.

A possible research stream for power's affect on information systems security policy compliance would be to view it from the lens as suggested by Jasperson et al. [17], which as stated above, is a model adapted from Bradshaw-Camball and Murray [6]. This would allow researchers to view power from the four different perspectives of rational,

pluralist, interpretive, and radical views. As suggested by Bradshaw-Camball and Murray, each view would uncover different explanations and descriptions. Used in various combinations, these views could assist researchers in an expansion in their knowledge on how information systems security policy implementations could become more successful.

The remainder of this paper is organized as follows. First presented is an overview of the power exercise conceptual framework as presented by Markus and Bjørn-Andersen [20]. This framework is then be used to create a model of the exercise of power by information systems security policy agents over employees. Subsequent to this, the model is applied to HealthCo to show how the stakeholders' awareness of power exercise can assist in improving the success of information systems security policy implementations. In the discussion section, the agent-employee dyad results are described with the model's assistance. Lastly, in conclusion, the model's applicability to both the practitioner and academic environments, is given.

III. IS PROFESSIONALS POWER EXERCISE CONCEPTUAL FRAMEWORK

Markus and Bjørn-Andersen [20] focus on the use of power in the user/information systems professional dyad. While intuitively one would think that information systems professionals have power over users because information technology is a resource that many people value, it has been purported that this is not necessarily the case [18][27][28]. These rewards (information technology) can be extracted from those who depend on it [24]. This power theory is "resource dependence" [25].

In their paper, Markus and Bjørn-Andersen [20] discuss the power of IS professionals over systems users and view this situation from a Jasperson et al. [17] interpretive power perspective. These authors purport that if both professionals and users can increase their awareness of the different types of power exercise, the quality of systems developed and the outcomes of their use, will be significantly enhanced. The framework they present looks at both the context of power exercise (specific development project or information systems management policy) and target of power exercise (issues of fact or issues of values). This framework is a matrix that gives the four types of power exercise: technical, structural, conceptual, and symbolic).

A technical exercise of power occurs when system designers select system design features to which users explicitly object, at least initially. A structural exercise of power occurs outside any specific systems development effort. A conceptual exercise of power, as well as symbolic exercise of power, deals with the users' values about, and attitudes towards, the issues of fact as the design features of systems and the distribution of access to computing equipment and services. The conceptual exercise of power links closely with the methods used to analyze organizational situations prior to developing system

design features. Information systems professionals exert power symbolically by shaping user's desires and values outside the context of an individual systems development effort.

Additionally, Markus and Bjørn-Andersen [20] looked at information systems professionals' and employees' awareness of power exercise. They suggest that having and using power are different. Power is often exercised without the knowledge of the actor or the receiver. This unawareness of power exercise occurs because people "seem to evaluate 'having power' differently from 'using power'" [20].

This awareness of power exercise results in four possible outcomes: 1) if both are aware then there is mutual negotiation, 2) if both are unaware then unintended influence occurs, 3) if the information systems professional is the only one aware, then professional manipulation occurs, and 4) with the reverse awareness level, user resistance occurs.

The exercise of power is not defined in the terms of intentions or the perceived legitimacy of outcomes; it is defined in terms of behavioral outcomes. The result of such a definition is that when information systems professionals have exercised power over the users then this is to say that the users behave differently than they would have if not for the professionals. This power over end-users can be collective or individual.

Hardy [15] and Lukes [19] use a similar definition of power exercise. However, there is some disagreement with this definition. A common alternate definition of the exercise of power, as that of Meyer [21], occurs only when the powerless individual views the powerful individual's behavior as illegitimate, or when the powerless does not accept their behavior. Additionally, Dahl [10] and Pfeffer [25] believe that the exercise of power only exists when the parties involved are not in agreement about a decision and where it is possible to view the powerful actor's behavioral attempts to influence the outcome of decisions. Both of these two alternatives are more restrictive and assume that the exercise of power is an intended action by individuals.

IV. INFORMATION SYSTEMS SECURITY POLICY POWER EXERCISE MODEL

This paper addresses the policy agent-employee dyad and specifically the power exercise of information systems security policy agents over the employees. It is suggested that with the mutual awareness of the different types of power exercise, the successful implementation of information systems security policy in organizations will improve. As stated, a successful implementation is defined as employee policy compliance.

An adaptation of the Markus and Bjørn-Andersen [20] framework of information systems professional power exercise to information systems security policy agents can be seen in Table I. So, in bridging from the Markus and Bjørn-Andersen framework, it is necessary to look at the target of power exercise (issues of fact or issues of values) and the context of power exercise (information systems security policy).

A. Target

Information Systems security power exercise can be directed at issues of fact and tangible resources. For instance, this may entail specific directives of the implementation plan like ‘all employees must attend a security 101 course’ or ‘each department will allocate \$300.00 per employee for physical security apparatuses such as locks.’ Additionally, an individual’s values may be taken into account. This may be values such as an individual’s acceptance of the

TABLE I
TYPES OF POWER EXERCISE

		Target of Power Exercise	
		Issues of Fact	Issues of Values
Context of Power Exercise	Specific IS Security Policy Category	Technical	Conceptual
	IS Management Policy	Structural	Symbolic

Adapted from Markus and Bjørn-Andersen [20]

objectives/reasons of a particular item in the implementation plan, the assessment of a policy’s success, the individual benefits of particular policies, cultural definitions of sound policy, or workplace institutionalizations [4].

B. Context

An information systems security agent’s ‘power exercise’ can also occur contextually. This can happen during activities such as when developing the implementation plan. In addition, power exercise can occur in the management policy environment around specific implementation specifics such as password use, password expiration, the mandated use of certain security applications like virus scan software, or the monies charged to departments to pay for information systems security policy classes.

As shown in Table I, the intersection of these two dimensions of target and context, produce four different ‘power exercises.’ These are Technical, Structural, Conceptual, and Symbolic. A definition of each, and its applicability to information systems security policy implementations are given.

C. The Technical Exercise of Power

The technical exercise of power occurs when policy agents identify specific ‘rules’ within a policy implementation plan which users explicitly object (at least initially). Even if users do not explicitly object to the policy implementation plan contents, the exercise of power has occurred if it is shown that users would have objected had they been aware of the agents’ identification of the plan content [19]. An example would be a policy that forces the use, and entry, of different passwords at multiple levels of applications, and the user’s desire is a password system that does not impeded their work (e.g., one password that is entered once).

D. The Structural Exercise of Power

The structural exercise of power is not as easily connected to the behaviors of individuals -- as the technical exercise of power can be. It occurs exogenous to any specific information

systems policy implementation. This is where the agents exercise power over user behavior by imposing organizational structures or instituting routine procedures that cause the garnered formal authority over users, or cause the user to be dependent on them for resources.

This may be something as simple as the stipulation that certain systems security software must be used, and additionally, must be purchased from an organization’s software store (where prices are set by the owned security organization). Alternatively, it could be more structurally relevant -- such as the information systems security agent may have other authoritative positions (e.g., overall approver for all information systems acquisitions like hardware and software). This power exercise deals with the development of implementation plans, not the application to a specific information systems security policy. When these structural constraints on users exist, they can unnecessarily render a need for more direct forms of power use (e.g., technical exercise of power).

E. The Conceptual Exercise of Power

This exercise of power is relevant to an individual’s values about, and/or attitude toward, the issues of specific way the security policy is implemented, the charges for security software, or even the exercise of power itself. As stated by Lukes [19]:

A might exercise power over B by getting him to do what he does not want to do, but he also exercises power over him by influencing, shaping or determining his very wants. Indeed, is it not the supreme exercise of power to get others to have the desires you want them to have—that is to secure their compliance by controlling their thoughts and desires?

An information systems policy agent may conceptually exert power over employees by developing the objectives of a specific information systems security implementation plan. Conceptual refers to the design concept of the information systems security implementation plan. This is the overall objective and purpose of the plan that ultimately (supposedly) contains the specific details of the implementation plan.

The conceptual use of power is closely connected with the method used to assess the organization prior to policy implementation (inclusive of the actual specifics of the plan). While the implementation plan may be quite rigid and structured, it also could be very loose and conducted haphazardly. The questions asked, or even more importantly not asked, may prevent the employees from expressing certain views (e.g., preferences, likes, dislikes) about the implementation plan specifics and objectives.

F. The Symbolic Exercise of Power

This is where the information systems security policy agents shape employees' values and desires, exogenous to the context of the policy implementation. This type of power exercise occurs while the employee actually comply with information systems security policies. So often on television, and in magazines, there are articles that talk about the importance of information systems security and the woes that could occur due to not being secured. There are reports of malicious catastrophes that occur which are based on information systems security [22]. From all of these reports, individuals realize that the results of not being secure could be devastating, and thereby these occurrences act as symbols. Therefore, when employees allude to the fact that information systems security policy is necessary to protect the company's assets, or their own, they are portraying the remnants of a subtle force of symbolic power exercise.

V. MODEL OF INFORMATION SYSTEMS SECURITY POLICY AWARENESS OF POWER

While there are four different types of power exercise, the proposed model does not assume that an awareness of the power exercise is necessary at any point in the process (before, during, or after) for the model to be applicable. Actually, neither party needs to be aware that power is being exercised. This really means that even if a policy agent is unaware that they are altering an employee's behavior, they may be, just by whom they are. It should be understood that power is exercised if there is a change in either the organizational outcomes (because, for instance, the presence of the information systems security agent), or the employee's behavior.

However, both the attributions of legitimacy and the awareness of power exercise can be relevant. They will affect how an employee responds to the information systems policy agent and their implementation specifics. Additionally, Markus and Bjørn-Andersen [20] purport that unawareness can move to awareness. "... we believe that interventions that increase this awareness will pave the way to compromises by opening up previously covert issues." This increase in awareness should lead to results that are more positive for the organization.

Table II shows the taxonomy of different conditions of awareness. Any one of these four situations may be present given an exercise of power. The upper left quadrant is 'Deal Making.' This occurs when both the information systems security policy agent and the employee are aware that power is being exercised, there is room for negotiation -- resulting in a 'win-win' situation. This is because each party is aware of the agent's power and they know what is conceivable and what is not. The bottom right quadrant is 'Blind Influence.' It is called this because when neither party is aware of the use of power then making a deal is slim; they just go with the program and whatever happens, happens.

The remaining two quadrants of the taxonomy bring the most difficulty as is explained by changes agents. The result is a win-lose situation, where the result benefits only one party. This is where the aware party can take advantage of the other party. When the information systems security policy agent is

unaware, and the employee is aware, they are 'Policy Dissenters' – at least this is how the agents view the employee.

TABLE II
AWARENESS ABOUT POWER EXERCISE

		Employee	
		Aware	Unaware
Information Systems Security Policy Agent	Aware	Deal Making	Policy Forcing
	Unaware	Policy Dissents	Blind Influence

Adapted from Markus & Bjørn-Andersen [20]

Conversely, when employees are unaware and agents are aware, the agent openly intends to influence unknowing employees – this is called 'Policy Forcing.'

VI. REVIEWING THE IMPLEMENTATION OF HIPAA AT HEALTHCO

This section analyzes the move within HealthCo to introduce the United States federally mandated HIPAA. The analysis is conducted using the power exercise model as described in the previous section of this paper.

A. Health Insurance Portability and Accountability Act of 1996

HIPAA was passed by the United States Congress on August 21, 1996. Congress included as part of this policy, regulations that promote the simplification of administrative health care transactions and those that ensure the security and privacy of patient information. There are four specific standards that are part of HIPAA: transaction and code sets, privacy, national identifiers and security [13]. All four standards are enforceable, with significant fines possible if the policies are not followed.

Of main concern are the privacy and the security policy of HIPAA in that both of these have security implications. The privacy policy set standards for the electronic financial and administrative transactions. The policy states that a party electronically maintaining or transmitting "protected health information," may not disclose or use the information except as permitted by federal regulation. Patients are also given the right to control how and when their information is used.

The confidentiality of health information is threatened not only by the risk of improper access to stored information, or the maintenance of that information, but also by the risk of interception during electronic transmission of the information. The security policy of HIPAA mandates the adoption of national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Prior to these rules, there were not any standard measures that existed in the health care industry that addressed all aspects of the security of electronic health information while stored, or transmitted, between entities (via either a local area or wide area network). Full compliance became mandatory on April 21, 2005. HealthCo, like all other health care organizations, were mandated by the federal government to follow the HIPAA policy guidelines.

HealthCo

For anonymity purposes, the actual names of the organization, and the employee names, have been changed. The descriptions of the roles and responsibilities have not been altered. HealthCo provides medical care to low-income and uninsured patients, as well as offers education to their patients. Services specifically provided are comprehensive reproductive health services, teen pregnancy prevention programs, family planning, breast and cervical cancer screening, mammograms, sexually transmitted disease testing and treatment, HIV/AIDS testing and counseling, colonoscopy, and peri- and post-menopause services; among other women's, men's, and teenagers' health programs. HealthCo's mission is to provide high quality, affordable reproductive health care; promote education programs that empower all individuals to make informed and responsible reproductive choices; and to protect the right to make those choices. HealthCo is an affiliate of a much larger parental organization that has branches throughout the United States. The affiliate HealthCo operates six offices in a major metropolitan United States city and employees 135 employees. These employees are either a member of the administration department or the clinic services department.

B. Case Study Description

This section describes activities and information that were gathered at HealthCo over a six month period. Data was gathered from records and notes made during meetings with employees of HealthCo over the six month period, as well as from artifacts that were provided by HealthCo employees (e.g., organization charts, mission statements, policy statements). A program log was kept containing a record of all discussions, both formal and informal. Three department meetings were attended and nine in-depth semi-structured interviews with employees from different areas of HealthCo were held. Of importance to this study, six individuals' contributions are presented to show the exercise of power and policy implementation at HealthCo. Three of these interviews were with individuals in the administration department and three who are in the clinic services department. During the in-depth interviews, open-ended questions were asked. Although a short list of questions was used to start an interview, other areas of inquiry were investigated based on the interviewee's points of discussion. The questions that were asked varied, but were mainly those that caused discussions about HealthCo, HIPAA, the rollout of HIPAA, the management, the information technology department, and those responsible for enforcing HIPAA in the organization.

Direct quotes from the interviewees are shown in italics. Figure 1 shows a partial organization chart that details the role of each employee highlighted in this paper.

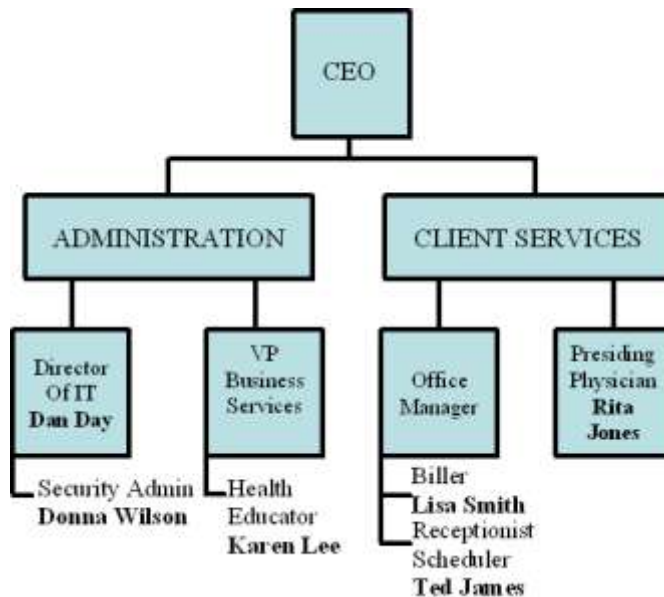


Fig. 1. HealthCo

C. Stakeholder Roles

The Director of IT, Dan Day, was given the responsibility of rolling out and enforcing HIPAA compliance at HealthCo. He was also responsible for HealthCo's overall information technology (IT) budget and ongoing IT expenditures. He reports to the CEO and she gave Day the authority to *make it happen*, no matter what it took. Making it happen meant that he, and his team, had to introduce HIPAA to the organization. Day and his team are management's agents. He was also responsible for enforcing employee compliance. During a staff meeting, where Day, Rita Jones, the office manager, and the VP of Business Services were present, the CEO made it clear that HIPAA violations would not be tolerated. She informed them that she gave Day the authority to *make it happen*. The CEO made it clear to her staff that an employee's employment at HealthCo would be in serious jeopardy if their non-compliance was discovered. The CEO informed her staff that violating HIPAA could possibly mean that HealthCo faced massive fines and penalties.

The authority that Day was given by the CEO gave him a lot of power in the organization; and he was aware of the power. Day was trained by Health and Human Services on HIPAA. Day stated:

A health care organization's non-compliance could have severe civil and criminal penalties... The CEO told me to make it happen. She didn't really care how I did it but she did say that she would even fire someone if they didn't follow the policy to the "t." I just need to let her know who isn't doing what they should be doing... I can also see what they do online and I had one of the technicians program the system so it made them have to change their passwords every 30 days. We never had anything like that before.

Day continued:

I think it is important but I don't like to manage with fear. You could tell a person to make sure that they locked their systems, or don't say a person's name on the phone out loud, or they may get fired. But what is that going to do? They would do it out of fear, rather than doing it because it's the right thing to do. I didn't tell Donna Wilson that the CEO said that she would fire somebody if they didn't follow the policy.

Wilson, who reports to Day, is the HIPAA security administrator. Since Wilson did not know that HIPAA compliance was one of the CEO's top priorities, to such an extent that a person could possibly be fired if reported, she was unaware of the power that she had. When asked to describe her role she said she was an educator and just sat down with people when they were hired and just described what HIPAA was. She also gave them a HIPAA pamphlet that she downloaded from the internet. Wilson had the responsibility for training new employees and the office staff, who reported to the office manager. The unfortunate part is that Wilson did not attend an external HIPAA training session, like her boss, Day. She was given a *train-the-trainer* session for about two hours on HIPAA by Day, and he did not inform her of the possible government penalties. One of the new people that Wilson trained was Ted James, the receptionist and scheduler, who reported to the office manager, who in turn reported to the CEO.

James was trained as a new employee and was oblivious to the healthcare environment. He had never worked in a hospital, a doctor or dentist's office, or a clinic prior to joining HealthCo. His role was to run the main HealthCo switchboard, route calls appropriately, and schedule client appointments. James did not know, understand, or seem to care about the power and politics that were present at HealthCo.

James iterates:

I just do my job. It's pretty straight forward. All the calls come into me and I forward them to the person. If they aren't there then they just go into voicemail. They don't go straight into voicemail, I was told, because of security reasons. They get a lot of treats here since this clinic performs abortions and they don't want people just getting through to anyone. I also schedule appointments here. [He opens up the office calendar and points to it. Revealed are clients' names and reasons for their appointments].

Jones is a doctor in the clinic and has been with HealthCo for six years. As the presiding physician, she reports directly to the CEO. Jones was quite aware of the importance of following HIPAA, and additionally, she knew of the possibility of large fines for non-compliance. She kept up with

her field and showed her level of understanding of HIPAA by stating:

HIPAA is the Act. It's a pain but it's important and you have to follow it. Patients don't want everyone knowing their personal information.

It is clear that the symbolic exercise of power in addition to legitimate authority was at play with Jones.

Karen Lee is a health educator. She reports to HealthCo's VP of Business Services, who reports to the CEO. The VP of Business Services knew the importance that the CEO placed on HIPAA; however, she did not stress its importance to her staff. Therefore, Lee was unaware of its priority at HealthCo and she did not know that repercussions were possible for non-compliance. Lee also did not deal directly with the IT organization, and therefore was unaware that Day signed off on all IT expenditures.

Lisa Smith is the billing administrator and reports to the office manager. As stated, the office manager reports directly to the CEO. At the initial rollout of HIPAA, the office manager informed her staff, including Smith about HIPAA. The office manager made it clear to Smith, and her colleagues, that HIPAA needed to be followed and that the CEO said it was important. Smith knew that if she was found to be in non-compliance, she could be terminated. She also knew that Day and Wilson were the HIPAA police, as her boss called them, and that Wilson was responsible for ensuring compliance of the office staff. Smith is clearly aware of the power and politics that the information systems implementation team has at HealthCo.

D. Discussion

Day, Jones, and Smith are very aware of the agent's power in implementing and ensuring the compliance of HIPAA at HealthCo. Wilson, James, and Lee are unaware of the power and politics that are occurring. Power and politics run rampant throughout HealthCo and affect the agent-employee dyads. Day knows that he has authority, given to him directly by the CEO. He also has power due to his information technology signoff authority. Wilson may not know that she has power, but she does. Her department is important to the organization and powerful as defined by the strategic contingency theory. Many other individuals in the organization know that compliance to HIPAA is mandatory at HealthCo.

As mentioned previously, Wilson is responsible for training and enforcing HIPAA compliance of all new hires, regardless of their position, and the office staff. Wilson is unaware of the power she has as the security administrator. Smith is quite aware of the power and politics in the organization and knows that she is supposed to comply. Unfortunately, even with knowing that she is supposed to comply, and additionally knowing that Wilson is responsible for enforcement, Smith states:

We have a lot of rules to follow... Since we have to change our password every 30 days and I can't for the life of me remember it. I just put it on a sticky and stick it here.

She points behind her monitor (out of sight of plain view) and then she smiles. As shown in Table III, Smith is a Policy Dissenter

TABLE III
AWARENESS ABOUT POWER EXERCISE AT HEALTHCO

		Employee	
		Aware	Unaware
Information Systems Security Policy Agent	Aware Day	Deal Making Day & Jones	Policy Forcing Day & Lee
	Unaware Wilson	Policy Dissents Wilson & Smith	Blind Influence Wilson & James

Wilson is also responsible for new hire HIPAA training and compliance. James, the receptionist was HIPAA trained by Wilson when he started. James is unaware of the power wield by Wilson or by IT. He does not fully comply with the rules of compliance either and in that he and Wilson are unaware of the power situation are in the Blind Influence stage (see Table III).

James said:

You know I've been a receptionist for a long time and I always learned that you acknowledge people by their name so I usually do – if no one is around my area listening. People want to be called by their name and acknowledged.

Day is responsible for training the Business Services department, of which Lee is a member. Lee is unaware of the power and politics at HealthCo. Since Lee is unaware of the power, and Day is aware, Day is 'Policy Forcing' and Lee does not comply (See Table III). She states in regards to passwords:

You're not suppose to use family members names because they say for security reasons somebody can figure them out. I just use my kids' and my husband's middle names and just add my address. Every once in a while you get locked out and you have to enter a new password. It won't let you enter a new one.

Day was also responsible for the training and ensuring compliance by the nurses and doctors. Since Jones was a member of the CEO's staff, she knew the power Day had. Not only did she know that a recommendation of termination to the CEO for non-compliance was possible, she also knew that Day approved the budget for IT and any interim IT expenditures. Her study outside of HealthCo, informed her of the importance of HIPAA and the ramifications possible. Table III shows that Day and Jones are 'Deal Making.' Jones says:

I know HIPAA is important, and I try to fully comply. There are a lot of rules but I try to stay up with them. A patients privacy is important and we need to keep their

information secure. People are really concerned about what people are finding out. Last week I read this article ...

VII. CONCLUSION

In this paper, the notions of power exercise and policy are used to present a new model of information systems security policy implementation. As was shown in the case study, an individual's awareness or unawareness of power exercise affects the outcome of an information systems security policy implementation. By raising the level of awareness of both the agents of information systems security policy, as well as the employees, there will be a mutual, consistent, effective, negotiated, and more efficient use of security policy.

From a practitioner's viewpoint, this research can assist in more effectively implementing information systems security policies. This can be done by ensuring that employees and policy agents in their organizations are aware of the exercise of power. They can also improve information systems security policy implementations and compliance by getting employees involved in the development, enforcement, and changing of the plans that are developed. This will in turn increase the employees' awareness levels of power use in the organization.

Policy implementation and power is a new research stream. With the many ways that researchers have purported that power and politics affects organizations, so too could these other power lenses be used to view information systems security policy implementations.

The limitations of this research present the future research possibilities. This research focused on the implementation of information systems security in organizations, purposely absent is looking at the development of these policies. Information systems security policy development can also be viewed from a power lens where the projected output is a security policy that is fair, manageable, and easily complied with by the entire organization. In addition, since as stated earlier, the awareness of power exercise does not exactly map to the types of power exercise, an exploration of the imperfect mapping of the two models is warranted.

While power is viewed in a variety of ways, it is important to see how it can be used to improve organizations, and specifically to increase the success rate of policy implementations. Clearly, the exercise of power, and more importantly the knowledge of such, is a vehicle in realizing this end. The optimal situation for an organization is where both the information systems security policy agent and the employee are aware of the exercise of power. If this is the case, they can mutually work together to make information systems security policy palatable for all.

REFERENCES

- [1] M.D. Abrams and D. Bailey, "Abstraction and refinement of layered security policy," in: *Information Security ± An Integrated Collection of Essays*, M.D. Abrams, S. Jajodia and H.J. Podell (eds.), IEEE Computer Society Press, New York, 1995.
- [2] W.G. Astley and P.S. Sachdeva, P.S., "Structural Sources of Intraorganizational Power: A Theoretical Synthesis," *Academy of Management Review*, vol. 9, no. 1, pp. 104-113, 1987.

- [3] R. Baskerville and M. Siponen, "An Information Security Meta-policy for Emergent Organizations," *Logistic Information Management*, vol 15, no. 5/6, pp. 337-346, 2002.
- [4] N. Bjørn-Andersen and D. Kjaergaard, "Choices en route to the office of tomorrow," in *Technology and the Transformation of White Collar Work*, R. Kraut (ed.), Erlbaum, Hillsdale, NJ, 1987.
- [5] P.M. Blau, *Exchange and Power in Social Life* John Wiley & Sons, New York, 1964.
- [6] P. Bradshaw-Camball and V. Murray, "Illusions and other Games: A Trifocal View of Organizational Politics," *Organizations Science* vol. 2, no. 4, pp. 379-398, Nov. 1991.
- [7] D. Buchanan and R. Badham, *Power, politics, and organizational change: winning the turf*, Sage Publications, Thousand Oaks, CA, 1999.
- [8] G. Burrell, and G. Morgan, *Sociological paradigms and organisational analysis: elements of the sociology of corporate life*, Heinemann, London, 1979, pp. xiv, 432 p.
- [9] S. Clegg, *Frameworks of Power* Sage Publications, Newbury Park, CA, 1989.
- [10] R.A. Dahl, "Power," in: *International Encyclopedia of Social Sciences*, D.L. Sills (ed.), The Free Press, New York, 1968.
- [11] G. Dhillon, *Managing Information Systems Security* MacMillan Press, London, 1997.
- [12] M. Foucault, *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977* Pantheon Books, New York, 1980.
- [13] S. Fuller, "Implementing HIPAA security standards - are you ready?," *Journal of the American Health Information Management Association* vol. 40, no. 9, pp. 36-40, Oct. 1999.
- [14] R.H. Hall, *Organizations: Structures, Processes, and Outcomes*, (7th ed.) Prentice Hall, Upper Saddle River, NJ, 1999.
- [15] D. Hardy, "The nature of unobtrusive power," *Journal of Management Studies*, vol. 22, no. 4, pp. 384-399, 1985.
- [16] D. Hickson, C. Hinings, C. Lee, R. Schneck, and J. Pennings, "A strategic contingencies theory of intraorganizational power," *Administrative Science Quarterly*, vol. 16, pp. 216-229, 1979.
- [17] J. Jaspersen, T. Carte, C.S. Saunders, B. Butler, H. Croes and W. Zheng, "Review: Power and Information Technology Research: A Metatriangulation Review," *MIS Quarterly*, vol. 26, no. 4, pp. 397-459, Dec. 2002.
- [18] J.H.C. Lucas, "Organizational Power and the Information Services Department," *Communications of the ACM*, vol. 27, no. 1, pp. 58-65, 1984.
- [19] S. Lukes. *Power: A Radical View* Macmillan, New York, 1974.
- [20] M.L. Markus and N. Bjørn-Andersen, "Power over users: Its exercise by system professionals," *Communications of the ACM*, vol. 30, no. 6, pp. 498-504, 1987.
- [21] M.W. Meyer, "Review of Power in Organizations," *Administrative Science Quarterly*, vol. 28, no. 2, pp. 301-303, 1983.
- [22] P.G. Neumann, "Risks to the public in computers and related systems," ACM SIGSOFT Software Engineering Notes, pp. 1-17, 1987.
- [23] Office for Civil Rights, "Summary of the HIPAA Privacy Rule," United States Department of Health & Human Services, Washington, DC, 2003.
- [24] A.M. Pettigrew, "Information Control as a Power Resource," *Sociology*, vol. 6, no. 2, pp. 187-204, 1972.
- [25] J. Pfeffer, *Power in Organizations* Pitman, Marshfield, MA, 1981.
- [26] R.S. Sandhu and P. Samarati, "Access control: principles and practice," *IEEE Communications*, pp 40-48, 1994.
- [27] C.S. Saunders and R.W. Scamell, "Intraorganizational distributions of power: Replication research," *Academy of Management Journal*, vol. 25, no. 2, pp. 192-200, 1982.
- [28] C.S. Saunders, C.S. and R.W. Scamell, "Organizational Power and the Information Services Department," *Communications of the ACM*, vol. 29, no. 2, pp. 142-147, 1986.
- [29] K.D. Schwartz, "Regulation Compliance Tops Companies' Security Concerns," in: *The Channel Insider*, 2004.
- [30] D.F. Sterne, "On the buzzword 'security policy'," Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 219-230, 1991.
- [31] J. Viega and J. Voas, "The pros and cons of Unix and Windows security policies," *IEEE IT Professional*, vol. 2, no. 5, pp. 40-45, 2000.
- [32] G. Walsham, *Making a World of Difference: IT in a Global Context* John Wiley & Sons, Chichester, England, 2001.
- [33] C.C. Wood, *Information Security Policies Made Easy*, San Rafael, CA, 1999.