Use Authorization

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at Idaho State University, I agree that the Library shall make it freely available for inspection. I further state that permission to download and/or print my thesis for scholarly purposes may be granted by the Dean of the Graduate School, Dean of my academic division, or by the University Librarian. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Signature ________________________________

Date ____________________________________

AN EVALUATION OF MOTIVATIONAL FACTORS FOR INFORMATION SECURITY POLICY BUY-IN

by

Eliot L. Long

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Business Administration in the College of Business

Idaho State University

Spring 2014

Committee Approval

To the Graduate Faculty:

The members of the committee appointed to examine the thesis of Eliot Lowell Long find it satisfactory and recommend that it be accepted.

Dr. Corey Schou,
Major Advisor

Dr. Mike McCardle,
Committee Member

Dr. Dorothy Sammons,
Graduate Faculty Representative

Table of Contents

List of Figures/Tables

Glossary

NOTE: The terms in this glossary have been copied and/or paraphrased directly from the sources indicated

Best Practice: Practices that have proven effective when used by one or more organizations and which, therefore, promise to be effective if adapted by other organizations (King 2000, 2)

Buy-in: The intent of an individual or organization to actively support a specified request ("English Definitions" 2014)

Compliance: The act of adhering to a specified request/requirement ("English Definitions" 2014)

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (*CNSSI-4009* 2006, 22)

Cyber Security: The ability to protect or defend the use of cyberspace from cyber-attacks (*CNSSI-4009* 2006, 22)

Escalated Privileges: Permissions higher than those authorized – For instance, a user having administrator access when they only have permission for user access has escalated privileges

Information: Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms (*DoD Instruction 8500.2* 2003, 19)

Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (*DoD Instruction 8500.2* 2003, 19)

Information Assurance Professional: Individual who works IA issues and has real world experience plus appropriate IA training and education commensurate with their level of IA responsibility (*CNSSI-4009* 2006, 35)

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (*CNSSI-4009* 2006, 37)

Information Security Policy: Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information (*CNSSI-4009* 2006, 37)

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (*CNSSI-4009* 2006, 37)

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information (*DoD Instruction 8500.2* 2003, 21)

Normative Beliefs: An individual's feelings regarding supervisor and coworker expectations that have been placed upon the individual (Siponen et al. 2006, 2)

Organization: A professional entity that maintains a structure and culture of employees ("Definitions and Meanings" 2014)

Perceived Severity: An individual's view of the harshness of the outcome due to the realization of a threat (Aurigemma and Panko 2012, 3253)

Perceived Vulnerability: The extent to which an individual views the likelihood of a threat coming to fruition (Aurigemma and Panko 2012, 3253)

Personally Identifiable Information: Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual (*DoD 5400.11-R* 2007, 9)

Procedure: A set of steps or methods for accomplishing a given task ("Definitions and Meanings" 2014)

Response Efficacy: An individual's feelings regarding how much compliance to the policy in question will benefit them (Ifinedo 2012, 84)

Security Posture: The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes (*CNSSI-4009* 2006, 67)

Self-efficacy: An individual's feelings regarding his/her ability to perform the tasks required by a policy (Ifinedo 2012, 84)

Subjective Norms: Refers to the value an individual places on the opinions of those close to him/her (Cheng et al. 2013, 452)

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (*CNSSI-4009* 2006, 75)

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source (*CNSSI-4009* 2006, 81)

AN EVALUATION OF MOTIVATIONAL FACTORS FOR INFORMATION SECURITY POLICY BUY-IN

Thesis Abstract – Idaho State University – 2014

Eliot L. Long, MBA

Supervisor: Corey D. Schou

Research has shown that information security policy (ISP) buy-in – the intent of an individual to comply with an organizations information security policy – is an important aspect every leader should strive to achieve; however, as recent highly publicized events such as the cases of Edward Snowden and Target have shown, policies are not being properly adhered to.. To further highlight the problem, an annual report by IBM indicates that 35% of all information security incidents and 31% of all information security breaches within organizations are due to employees demonstrating unauthorized access, suspicious activity, and/or access/credential abuse (*IBM Security Services* 2013). These incidents and breaches come from employees not buying into ISPs, thus undermining information security efforts.

Prior research has shown that an individual's perceptions and beliefs have a direct relationship on ISP buy-in. However, that relationship is not enough as leaders may use motivational tools to enhance this relationship and lead their employees toward higher levels of buy-in. For instance, the use of a negative incentive, such as the threat of being fired, alters an employee’s perception regarding the costs associated with ISP noncompliance. On the other hand, the use of positive authority such as the encouragement of the employee influences the employee’s belief in his/her ability to comply with the information security policy. In both cases, the use of a tool impacts the strength of the relationship between perceptions and beliefs and ISP buy-in. By understanding the motivations of their employees, leaders may utilize tools to further influence ISP buy-in. This thesis proposes a new model illustrating this addition of motivational tools to increase the level of information security policy buy-in within organizations, both federal and non-federal.

Chapter 1: Introduction

Information systems (ISs) such as computers, smartphones, tablets, etc., have become pervasive within almost every aspect of the day-to-day lives of individuals around the world. For instance, ISs can regulate insulin in an individual’s diabetic regulator as well as help develop military combat strategies. As a result of this pervasiveness, countries have witnessed a rise in threats against ISs and also a rise in policies regarding the protection of those ISs, and the information they handle, from those threats. Within the United States in particular, many government entities and private corporations now maintain information security policies (ISPs) such as acceptable use policies in order to provide guidance for the protection of information and information systems. Information security policies are those sets of rules and acceptable practices as outlined by an entity regarding the management, protection, and distribution of information (*CNSSI-4009* 2006). In other words, ISPs outline the acceptable practices and procedures by which employees are expected to adhere. Without employee buy-in regarding these policies, those boundaries are violated and the potential for a breach in information security is high.

Increasing information security policy buy-in and thus reducing the potential for breaches in information security is not a simple task. The literature suggests that employee perceptions and beliefs serve as the motivation for ISP buy-in. As these perceptions and beliefs are inherent to employees, this thesis asserts that leaders have the means of enhancing an employee’s motivation toward ISP buy-in through the use of tools such as incentives, capacity-building, and authority. As a result, this thesis answers the following research question: How can leaders motivate their employees to buy into ISP?

Importance of Research

The issue of information security policy buy-in is ever present in today's society and exists within entities such as federal and state governments as well as within corporations. While this thesis focusses on the governmental side, the concepts presented are also applicable to corporations as well.

ISP buy-in is important because the strength of an organization's information security can be degraded if employees do not follow the policies. For instance, a lack of employees buying into ISP is illustrated in an annual report by IBM showing the results of a survey conducted across 130 countries. Within this report, IBM found that 35% of all incidents and 31% of all breaches within an organization are due to employees demonstrating unauthorized access, suspicious activity, and/or access/credential abuse (*IBM Security Services* 2013). Additionally, a report from the Department for Business Innovation and Skill in the UK supports these findings for the UK specifically (*2014 Information Security Breaches Survey* 2014). As such, a significant lack of ISP buy-in is clearly present across the world, creating a weakness in information security.

This issue of noncompliance with ISP becomes extremely significant as even the smallest weakness has the potential to infect the entity as a whole. In this case, the employees causing such high rates of incidents and breaches create a potential opening for malicious actors to enter organizational systems. Malicious actors may then use this entry point to gain access to information within the network. If employees were to buy into and comply with ISPs, these types of weaknesses could possibly be reduced.

In addition to the incidents mentioned by IBM, the United States Government (USG) in particular has been faced with a violation of information security in the form of the highly publicized incident involving Edward Snowden's coworkers. Snowden obtained unauthorized access to classified documents through a number of means including through the use of coworker credentials by convincing them to share their credentials with him (National Security Agency 2014). By sharing their credentials with Snowden, the coworkers violated the agency's ISP that no individual was to share private/personal credentials with any other individual; which resulted in Snowden obtaining unauthorized access to a number of the documents he would later release. Had the coworkers bought into the agency's policy to not share credentials with other individuals, Snowden's damage would have been limited as he would have been required to find alternate violations of information security policy to leverage.

Snowden's coworkers willfully non-complied with the agency policies they agreed to uphold and a breach in national information security was the result. According to the McCumber model – a model developed as a basis for information security – there are three countermeasures to help protect against a security violation: policy, people, and technology (McCumber 2005). In the case of Edward Snowden, though the technology was sufficient, he found ways to violate the law by leveraging his coworkers' lack of ISP buy-in. It is the lack of buy-in from individuals such as Snowden's coworkers that this thesis looks to address.

Leaders need to learn from these types of failure in ISP buy-in in order to build stronger means for detecting and preventing policy noncompliance. One method of accomplishing this is through employee motivation across many disciplines and functions. Leaders are responsible for embracing all disciplines of ISP – organization wide, incident specific, and system specific ("Information Security Policy" 2006) – and ensuring that they include considerations for the organization's culture and security risks (Hinde 2002). In doing this, leaders may then use tools as means for motivating the buy-in of these information security policies.

To effectively utilize motivational tools, leaders must first acquire a certain level of power from their employees. French and Raven (1959) present five forms of power available to leaders: coercive (the leader forces his/her employees to complete a task), reward (the leader presents positive outcomes for his/her employees), legitimate (the leader holds power based on his/her status in the organization), referent (the leader's subordinates have given him/her power over them), and expert (the leader is given power based on his/her technical expertise). Of these five forces of power, the strongest force is that of referent power. With referent power, the leader is followed because his subordinates believe in him/her as a role model and thus desire to follow the leader rather than being required to follow the leader. Having referent power instills strong motivation in subordinates and brings them toward a common goal (French and Raven 1959).

Leaders may pair this influence from referent power with strong motivational tools to assist them in generating motivation within their employees. By motivating employees in such a way, an organization will have a better ability to strengthen its assets and bring its employees together toward the common goal of information security policy buy-in.

To move closer to achieving this goal of ISP buy-in, this thesis discusses information security policies as a focus toward which organizational leaders should apply motivational tools. Chapter 2 below contains a discussion on ISP in the terms of relevant Acts that have helped to mold the development ISPs. This is then followed by a discussion on motivation in terms of motivational theories and models that set the basis for motivating employees toward ISP buy-in. The thesis uses these theories and models to set the stage for a new model that incorporates motivational tools as enhancements to the relationship between employee motivation and ISP buy-in.

Chapter 2: Literature Review

In this chapter, the base for the model proposed in Chapter 3 is established. In order to understand how the proposed model will help influence ISP buy-in, it is important to first understand information security policy and motivation within information security.

Information Security Policy

As stated previously, ISP is defined as those sets of rules and acceptable practices as outlined by an entity regarding the management, protection, and distribution of information (*CNSSI-4009* 2006). This definition suggests that policies lead to procedures which ultimately lead to the best practices for the security of information. Think of an information security policy as the foundation of a building and the procedures and best practices as the walls. One must build the walls on a strong, solid foundation or the walls will begin to crack and collapse. While there will always be weaknesses in every foundation, it is the duty of leaders to guide their employees toward reducing weaknesses by providing information security.

To ensure information security, leaders need to look to information security policy as the beginning to effective security management. ISP acts as a bridge between executive and departmental levels of an organization and should be infused into the inner workings of that organization. In accomplishing this integration, consistency is developed within the organization, helping to reduce weaknesses in that organization's security posture (Higgins 1999). This consistency is the goal of any ISP and can only be accomplished if employees adhere to policy.

To establish consistency and reduce security weaknesses, ISPs define acceptable and unacceptable behavior within an organization and serve to enforce information security laws and best practices. Without the boundaries set by the laws and best practices and the policies to enforce them, organizations would potentially fail to maintain structure and consistency in secure operations across departments (Whitman 2008). Laws, also known as Acts, which helped to mold information security policy are discussed below.

Information Security Acts

This section provides a sampling of the Acts that drive information security policy. Acts such as those that follow provide a basis for ISP creation and thus are the first step in understanding the concerns addressed within ISP. Without these Acts, information security policy would not necessarily have been molded to focus on the aspects of protecting information in the same way it does today.

Computer Security Act of 1987 (CSA)

The Computer Security Act of 1987 (CSA), also known as Public Law 100-235, was passed to coordinate the development of security standards by providing agencies with computer security through the use of personnel training regarding secure practices for the management, operation, and use of USG computer systems (Congress 1988). In other words, the CSA established the requirement for any employee who comes in contact with federal information systems to receive education regarding the acceptable practices for handling those systems. This Act was written as a means for requiring information security initiatives, such as this type of training program, to be implemented within the Federal Government (Congress 1988).

The CSA was enacted as a result of the U.S. Congress recognizing the need to make advances in the privacy and security of the nation's "sensitive information." Specifically, it was written to set an acceptable level for procedures protecting Federal computer systems without reducing the breadth and depth of security practices already in place at the time. The CSA states distinct goals including the institutionalization of plans regarding the security of systems containing sensitive information as well as the mandating of periodic security training programs for employees handling sensitive information (Congress 1988).

The Computer Security Act of 1987 remains in effect today and was the nexus for follow-on Acts relating to information security. In requiring the education and training of employees, this Act established expectations for employee interaction with Federal information systems. The CSA was one of the first Acts setting the foundation for information security policy (ISP) to build upon. As these ISPs were developed, issues relating to the need for compliance arose. As such, the CSA ultimately became one of the first Acts that laid the groundwork for the need for ISP buy-in.

Federal Information Security Management Act of 2002 (FISMA)

The Federal Information Security Management Act of 2002 (FISMA), also known as Title III of the E-Government Act of 2002 and Public Law 107-347, was enacted as a way to recognize the significance of needing information security within U.S. national and economic security interests. Under the scope of FISMA, federal agencies are required to "develop, document, and implement" programs offering information security to protect agency assets supporting information and information systems. This includes any assets handled by other agencies, contractors, etc. ("Federal Information Security" 2014). In other words, FISMA is similar to the Computer Security Act of 1987 in the fact that it requires education programs for any individual who wishes to come in contact with a Federal information system. However, FISMA takes the CSA a step further and requires agencies and contractor companies to maintain specified levels of security on the information systems handling sensitive information.

To accomplish the tasks outlined in FISMA, the National Institute of Standards and Technology developed the FISMA Implementation Project, which created several information security standards and guidelines that the legislation mandated ("Federal Information Security" 2014). A list of initial publications developed under this project is found in Appendix A, Exhibit 1. Of particular note is FIPS 199, which made the implementation of FISMA mandatory. Prior to FIPS 199, it was simply suggested that agencies adhere to the standards set in FISMA. However, post FIPS 199, these standards became a requirement for agencies to follow; resulting in agencies developing FISMA related ISPs.

Through the Implementation Project, FISMA was intended to help establish cost and risk focused information security programs. Additionally, federal agencies and contractors were and still are expected to carry out a certain level of due diligence in the securing of information and information systems. The idea is that out of this due diligence will rise more efficient and effective security control applications and assessments as well as a higher level of comprehension regarding mission risks involving information system operations. The ultimate goal of FISMA is to create higher quality information to enable decision makers to make more informed information security judgments, thereby helping to create a critical infrastructure composed of more secure information and information systems ("Federal Information Security" 2014).

FISMA places importance on risk-based policies focusing on cost-effective security. To support this Act, the Office of Management and Budget (OMB) Circular A-130 Appendix III, *Security of Federal Automated Information Resources*, dictates that executive federal agencies are to plan for security by assigning proper responsibilities to specific roles and by conducting periodic reviews of security controls ("Federal Information Security" 2014).

In other words, FISMA assigns accountability for ISP violations and creates a framework for setting effective security controls. This framework charters the office of the Chief Information Officer to develop and maintain policies and procedures and to determine specific controls to be utilized for specific types of information. The accountability established under FISMA creates a means for security policies to be developed. Similar to the Computer Security Act, FISMA creates a foundation for ISP development and with ISPs comes the requirement for compliance and the need for buy-in.

Committee on National Security Systems (CNSS)

In addition to the federal Acts discussed above, the United States Federal Government has the Committee on National Security Systems (CNSS).. The CNSS is given the authority to establish Information Assurance policies, procedures, instructions, etc., regarding the protection of National Security Systems (NSS). Also, the CNSS is responsible for offering a forum for discussing policy issues. This forum allows for the collaboration among agencies to assist in the unification of ISPs across these entities. The Committee is tasked with ensuring the protection of NSS against exploits by offering the following ("Committee on National Security Systems" 2014):

- A technical foundation within the USG, setting a standard for the information systems that process, store, and transmit NSS
- Support from the private sector to assist the technical foundation within the USG
- Continued/reliable assessments of vulnerabilities and threats
- The implementation of effective countermeasures against those vulnerabilities and threats

The CNSS is intended as a means of increasing communication and collaborations amongst governmental communities. Specifically, the CNSS spans the Intelligence Community, Civil Agencies, and Department of Defense. The reason for this goal of lowering borders between communities is because the creators of the CNSS recognized an increasing threat to the United States cyber environment (“Committee on National Security Systems” 2014).

Over the years, the CNSS has become the foundation for information security guidance and collaboration efforts across agencies and corporations (“Committee on National Security Systems” 2014). Vulnerabilities and threats are constantly changing; therefore, collaboration between the public and private sectors is necessary to provide more effective information security for the nation. Through the promotion of guidance and collaboration amongst these entities, the CNSS helps establish a cohesive environment that fosters ISP buy-in.

Additional Acts

In addition to the Acts and Committee mentioned above, there are more specific Acts that pertain to corporations. A summary of each Act is given along with an assessment of how they relate to information security policy buy-in. Appendix A, Exhibit 2 briefly presents six pieces of legislation considered to be relevant for organizations doing business in varying industries such as the financial, healthcare, and credit card industries ("Regulatory Compliance Demystified" 2006).

Sarbanes-Oxley (SOX)

Sarbanes-Oxley (SOX), also known as Public Law 107-204, was enacted in 2002 partly due to the financial scandals of Enron in 2001. Sarbanes-Oxley was written as a control on publicly traded organizations requiring the confidentiality and integrity of financial data, thus allowing for a level of investor confidence. Section 404, “Management assessment of internal controls,” is essential for developers working with financial systems. As part of Section 404, management is made responsible for taking due diligence in the evaluation of IT systems and processes that handle information that may be considered sensitive. While Sarbanes-Oxley does not refer to information technology directly, IT is affected in the fact that financial data is often handled by IT systems ("Regulatory Compliance Demystified" 2006).

Section 302 of SOX directly affects information security in the fact that it holds executives accountable for the systems under them. It requires CEOs and CFOs to attest to the sufficiency of financial controls. Consistent external audits on these controls must be conducted in order for an organization to obtain/retain SOX compliance. As a result of this, substantial investments have been made in the area of IT and information security ("Regulatory Compliance Demystified" 2006).

Assuming that the CEOs and CFOs that are held accountable for SOX compliance want what is best for their organizations, they must buy into the Act and its resultant policies to maintain their business operations. Many of these executives will have referent power as mentioned in Chapter 1, meaning that their buy-in will motivate the employees of their organizations to also buy into the company policies relating to the Act.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), also known as Public Law 104-191, was enacted in 1996 as a requirement for entities to meet a standard level of security if they handle electronic protected health information (ePHI). This act was written with the intent of being a foundation for entities to build upon rather than as a ceiling. In other words, organizations handling ePHI must meet HIPAA at a minimum; however, they are still encouraged to go above and beyond ("Regulatory Compliance Demystified" 2006).

Under the umbrella of HIPAA, ePHI regulations are required to be applicable across all levels of an affected organization. As a result, HIPAA regulations are intentionally ambiguous. However, the Act does list three specific types of safeguards as requirements: administrative, physical, and technical. Administrative safeguards are those dealing with business continuity. For example, disaster recovery plans and contingency plans would fall under the category of administrative safeguards. Physical safeguards deal with exactly what the name suggests: physical controls such as guards, gates, and other forms of access controls. Technical safeguards deal with information being stored, processed, and/or transmitted within the organization’s ISs ("Regulatory Compliance Demystified" 2006).

Along with the three safeguard categories specified within HIPAA comes the need for policies implementing and maintaining the safeguards. For instance, disaster recovery and contingency plans under administrative safeguards need policies and procedures to establish roles and responsibilities for employees in the event of a disaster. Without these policies, employees would be at the mercy of the organization’s own guidelines for handling such incidents rather than having the consistency that accompanies an Act such as HIPAA.

HIPAA compliance also requires policy buy-in from the employees. If an employee rejects the roles and responsibilities assigned to him/her through the policies developed in response to the Act, then those policies become ineffective as another employee that may not have the appropriate knowledge and training for that role must now attempt to fill the position in the event of an incident. Administrative, physical, and technical safeguards can apply to all employees in any industry and not just to those that fall under the scope of HIPAA. Therefore, policy buy-in for these safeguards is essential for any organization’s information security.

Payment Card Industry (PCI) Data Security Standard

The Payment Card Industry (PCI) Data Security Standard sets standard requirements for any organization that deals with transmission, processing, and storage of cardholder data. The PCI Data Security Standard requires the employees of any entity that handles credit card transactions/data in this way to encrypt the data so as to protect its contents from unauthorized individuals. These employees are subject to PCI Data Security Standard compliance covering the areas of systems, policies, and procedures for the protection of credit card data ("Regulatory Compliance Demystified" 2006).

Just as HIPAA requires safeguards and employee buy-in for the protection of healthcare information, the PCI Data Security Standard has requirements to protect credit card transaction information. Anyone who has been a victim of identity theft like the recent breach in Target's security in 2013 can attest to the importance of this standard. The incident involved the compromise of numerous customer credit card transaction data, including account numbers and passwords. The author of this thesis has firsthand experience with the ramifications of this breach. The employees working for the company providing Target with its point of sale credit card systems may not have bought into and followed the policies created under the PCI Standard, thus allowing thieves to steal customer transaction data. Had the systems been protected according to the policies developed under this Standard, such an incident may not have occurred..

Gramm-Leachy Bliley Act (GLBA)

The Gramm-Leachy Bliley Act (GLBA) was enacted "to facilitate industry-wide financial services reform." It was presented as a means for offering a common framework for banks, security firms, financial service providers, etc. and was intended to dissolve the barriers blocking the merge of financial institutions ("Regulatory Compliance Demystified" 2006).

The GLBA makes directors and CEOs personally and financially accountable for the misuse of the personally identifiable information of customers. Noncompliance with the provisions set in the GLBA results in a minimum of monetary fines ("Regulatory Compliance Demystified" 2006). Revisiting the Target example from under the PCI Data Security Standard section, Target's CEO was held accountable for the breach in security and ultimately "resigned" from his position as a result (D'Innocenzio 2014).

When individuals feel personally and financially responsible for something, they tend to be more invested in its success. CEOs have legitimate power based upon their position in the organization. By making CEOs personally accountable for misuse of personally identifiable information, they will enforce the policies with their subordinates, forcing compliance. Hopefully, the CEO will obtain referent power and foster an environment of buy-in of the GLBA within their organizations. Increased compliance and buy-in means increased security of citizen information.

California Security Breach Information Act of 2003 (SB 1386)

A final relevant policy is California Security Breach Information Act of 2003 (SB 1386). This bill requires all individuals and/or organizations maintaining personally identifiable information as well as conducting business within California to protect the personally identifiable information of customers. The bill defines personally identifiable information as an individual's first and last name as well as their driver's license/California ID card number, financial account information, and/or social security number ("Regulatory Compliance Demystified" 2006).

A company is considered to have violated SB 1386 if it has at least one of the items listed above in an unencrypted format. However, if the piece of personally identifiable information is openly accessible through a separate, public resource other than the organization in question, then the organization is not required to encrypt the information within its systems ("Regulatory Compliance Demystified" 2006).

This loophole of possibly remaining compliant even if the information is unencrypted in organization systems could pose a threat to ISP buy-in. If an employee within the organization knows that the information is publically available through another source, he/she may no longer care about the protection of that information. For instance, if an employee were able to find a customer’s ID number in a public database, he would not be required to protect that information. Knowing this, the employee may now spend his/her efforts searching out the other personal identifiers covered by ISPs written in response to SB 1386 rather than working to actually protect that data, thus shifting the focus away from the ISP and toward the loophole instead. Having an opening such as this could potentially undermine compliance efforts with SB 1386 and thus reduce the buy-in of policies relating to such an Act.

Acts such as the ones discussed above are the law and set the foundation for the establishment of information security policies. One goal of information security policies is to uphold these laws as well as to provide employees with clear means for understanding what is expected of them within the law. However, the development of ISPs is not enough. Leaders must drive employees to buy into information security policies. One way to do so that has been examined in the literature is through the use of motivation.

Motivation

Motivation is an important part of being able to assess people’s level of ISP buy-in. Motivation is driven by an individual’s perceptions of their environment and their internalized beliefs (Harpine 2008). According to Maslow (1943), motivation does not indicate actual behavior; rather, it influences actual behavior. In other words, motivation answers the “Why?” of actual behavior, not the “How?” (Ryan and Deci 2000).

In examining why an individual acts the way he/she does, Maslow argues that individuals are motivated based upon internal and external factors (Maslow 1943) which are referred to as being intrinsic and extrinsic. Intrinsic motivation occurs through an individual’s passion for a task, while extrinsic motivation occurs out of an individual’s desire for some specific outcome (Usher and Kober 2012). For instance, an employee who has a passion for information security will be intrinsically motivated to buy into ISP, while an employee who has ISP forced upon him/her can be extrinsically motivated to buy into the policy if he/she desires to receive a benefit or avoid a penalty.

Understanding these factors is essential for leaders as they must motivate their employees for their organizations to survive. Also, they must recognize that every employee is different and may require alternate forms of motivation to buy into a policy than those forms of motivation that other employees may require (Lindner 1998). Information security policy buy-in efforts need to focus on both intrinsic and extrinsic factors on the individual level.

These factors may be regarded as the individual’s perceptions and beliefs. The perceptions of the individual result in how that individual views compliance with the information security policy in question (extrinsic motivation). The beliefs, on the other hand, fall much more closely to the core of the individual as they are the internalized feelings the individual has regarding ISP compliance (intrinsic motivation). Both constitute the core of an individual’s motivation to carry out an act. Therefore, leaders must work to shape both perceptions and beliefs to motivate employees toward information security policy buy-in. These perceptions and beliefs have been characterized within the motivational theories discussed in the following section.

Motivational Theories

Throughout the years, many studies have been conducted regarding ISP compliance. Within these studies are behavioral/motivational theories that underlie human intent to comply (i.e., ISP buy-in). Upon researching the studies, at least four specific theories – Protection Motivation Theory (fear), General Deterrence Theory (penalty), Theory of Planned Behavior (intent), and Social Control Theory (relationship) – focus on an individual's perceptions and beliefs and have been identified as relevant for motivating policy buy-in. As such, a short background discussion on each follows.

Protection Motivation Theory

Protection Motivation Theory (PMT) was developed to explain appeals of fear. Many studies have shown fear to be an unpleasant emotion that individuals will work tirelessly to avoid. These same studies have determined that the desire to avoid fear is a strong factor in motivating employees to comply with a task, especially if they are given an avenue to reduce such fear (Norman et al. 2005). Therefore, Protection Motivation Theory is an ideal theory to assist in the examination of information security policy buy-in as the avenue presented to employees is that of ISP compliance, thus helping to reduce the fear of punishment.

To address their fear, an employee assesses a threat and attempts to cope with that threat. In the first element of PMT, assessing the threat, the individual reacts based upon his/her perception of the vulnerability and his/her perception of the severity of the penalties (Ifinedo 2012). In other words, an individual behaves based upon both the probably he/she views of the threat coming to fruition due to noncompliance and the perceived severity of the costs that result from the threat becoming a reality. For example, an employee may falsify expense reports to claim more expenses than actually occurred. If a company has a policy to terminate the employee for falsification of expense reports, then this threat of termination may deter the employee from falsifying the records. However, if the employee believes that the expense reports are not appropriately reviewed by the company, the perception of being "caught" is low; and the perceived severity of the costs that result from the threat (termination) becoming a reality are low as compared to the immediate benefit of additional expense reimbursement. In terms of ISP buy-in, the employee that perceives the risk of being "caught" for unsecure practices such as the sharing of credentials to be low will be more inclined to violate the ISP than the employee that perceives this risk to be exceptional.

The second element of PMT deals with how an individual copes with the perceived threat. This is known as coping appraisal and is considered an individual's conscious reaction to handling a threat (Rippetoe and Rogers 1987). In other words, coping appraisal is how an individual decides to react to a threat. In the example above, the employee that perceives the threat as low ignores the risk; however, the employee that perceives it to be high consciously avoids falsifying the expense reports in order to avoid the threat.

This conscious reaction is comprised of the individual’s belief in his/her ability to carry out the required behavior, the individual’s perception that the required action will create some sort of benefit for himself/herself, and the individual’s perception of the extent of that benefit.   (Ifinedo 2012). For instance, an employee that believes he/she lacks ability and/or perceives a high cost to complying with an ISP, with little benefit, will not be as likely to buy into the policy as an employee that believes in his/her ability to comply with the policy and/or understands the protective benefit the ISP provides to his/her own security.

The incident, as mentioned in Chapter 1, with Snowden’s coworkers is the perfect example of PMT. The employees did not perceive the risk of being caught for a violation to be great and thus proceeded to violate the ISP to not share credentials. All in all, Protection Motivation Theory looks into the individual’s perceptions of the costs/risks of not complying with an information security policy, thus influencing that individual’s buy-in relating to the ISP.

General Deterrence Theory

General Deterrence Theory (GDT), holds that an individual is deterred from certain behaviors based upon his/her perceptions of the penalties (Herath and Rao 2009). The penalty for committing an unsatisfactory act must be comprised of the following three characteristics: certainty, speed, and severity (Williams and Hawkins 1986). For instance, an employee decides whether or not to comply with an ISP based on how he/she believes he/she will be punished for noncompliance. Similar to Protection Motivation Theory, if the individual believes that the organization will simply overlook the violation, then he/she is more inclined to commit the violating act; however, if the individual believes that he/she will be reprimanded and/or suspended within the next 24 hours for instance, then he/she may be deterred from noncompliance with the policy.

General Deterrence Theory takes PMT one step further by making three key assumptions: legality, perception, and subjectivism. The legality assumption holds that there must be a set, known structure of boundaries outlining compliant and noncompliant behavior (Thornton et al. 2005). The perception assumption asserts that an individual perceives a certain level of threat regarding the punishment accompanied by noncompliance. Finally, the subjectivism assumption holds that each individual will maintain different beliefs that impact his/her perceptions regarding a punishment. What these three assumptions are stating is that each individual will view a punishment in different ways. One employee may perceive low legality/standardization of penalty and high threat while another employee may perceive just the opposite or some other combination of thereof.

By combining these three assumptions with the required characteristics (certainty, speed, severity) of a penalty, an individual determines whether or not it is beneficial for him/her to carry out a specific task (Williams and Hawkins 1986). For example, an employee who understands the benefits from ISP compliance that lead to his/her continued employment, and to the continued existence of the organization, as well as perceives the penalty associated with noncompliance will be more likely to buy into the policy than an employee who neither understands these benefits nor perceives the penalty for noncompliance.

Theory of Planned Behavior

The Theory of Planned Behavior (TPB) suggests that behavior is determined by an individual’s intent to perform a specific action. This intent is believed to encapsulate the motivational aspects that affect behavior (Hu et al. 2012). This theory holds that behavior is affected by three variables: attitude, subjective norms, and perceived behavioral control. Attitude is an individual’s emotions toward behaving in a particular way (Ajzen and Driver 1991). In other words, attitude is another way of stating whether or not an individual wants to perform a specified action. Subjective norms are defined as how an individual perceives how those close to him/her feels about the behavior in question (Ifinedo 2012). Does the individual feel as though he is expected to follow the ISP or that his/her friends and family will view him/her poorly if he/she does not comply? Finally, perceived behavioral control relates closely to self-efficacy from Protection Motivation Theory in that it refers to the individual’s perception regarding the level of difficulty for performing a specific task (Ajzen 1985). Another way to look at perceived behavioral control is to view a task in terms of updating an organization’s computer systems. An individual who views the task of ISP compliance to require him/her to physically log into and manually update every system within the organization may be less willing to buy into the policy than an employee who views compliance to require a simple push of a button that propagates the updates to all systems.

Researchers have incorporated the Theory of Planned Behavior in their examinations of an individual’s intent to comply with ISP. The studies performed by these researchers have shown that this intent is influenced by the three variables (attitude, subjective norms, and perceived behavioral control) presented within the TPB. It is through the perceptions and beliefs underlying this theory that intent to perform specific behaviors, and thus buy into ISP, is derived (Bulgurcu et al. 2010).

Social Control Theory

Social Control Theory holds that an individual assesses a situation based upon the maximization of pleasure through relationships with others (Hirschi 1986). SCT states that an individual maximizes this pleasure through deterrence from unacceptable behavior by the boundaries created from social structures. An individual who maintains a strong bond with his/her peers and/or superiors will be less likely to perform unacceptable actions (Cheng et al. 2013). For instance, an employee who enjoys going to work and views his/her supervisor as a role model will want to foster his/her relationship with his coworkers and will avoid behaviors that jeopardize that relationship.

Social Control Theory is similar to the subjective norms from TPB in the fact that it deals with an individual's perceptions and beliefs as they relate to other individual's. However, SCT enters into more detail by maintaining that there are four characteristics to any social bond: attachment, commitment, involvement, and belief. Attachment refers to the strength of the bond an individual feels toward "significant others." Commitment refers to the individual's desire to obtain a positive reputation with his/her peers. Involvement refers to the time an individual invests in his/her commitment to others. Finally, belief refers to the level of acceptance an individual holds toward socially acceptable behavior (Cheng et al. 2013). The stronger these four characteristics are within an individual's social bonds, the more likely the individual is to comply with an organization's information security policies (Junger and Marshall 1997). For instance, an employee who is strongly committed to and involved in the implementation team for ISP will feel as though he/she has an investment in that team and will want to align his/her goals to its goal of ISP compliance, thus increasing the level of that employee's buy-in. On the other end of the spectrum is the employee who lacks an investment in the implementation team. This employee begins to attempt to avoid working with the team and could possibly even attempt to undermine its efforts in an attempt to have punishments inflicted on his/her teammates. This ultimately undermines the entire compliance effort and increasing the barriers to compliance, thus altering teammate perceptions and beliefs regarding the ISP and possibly reducing ISP buy-in.

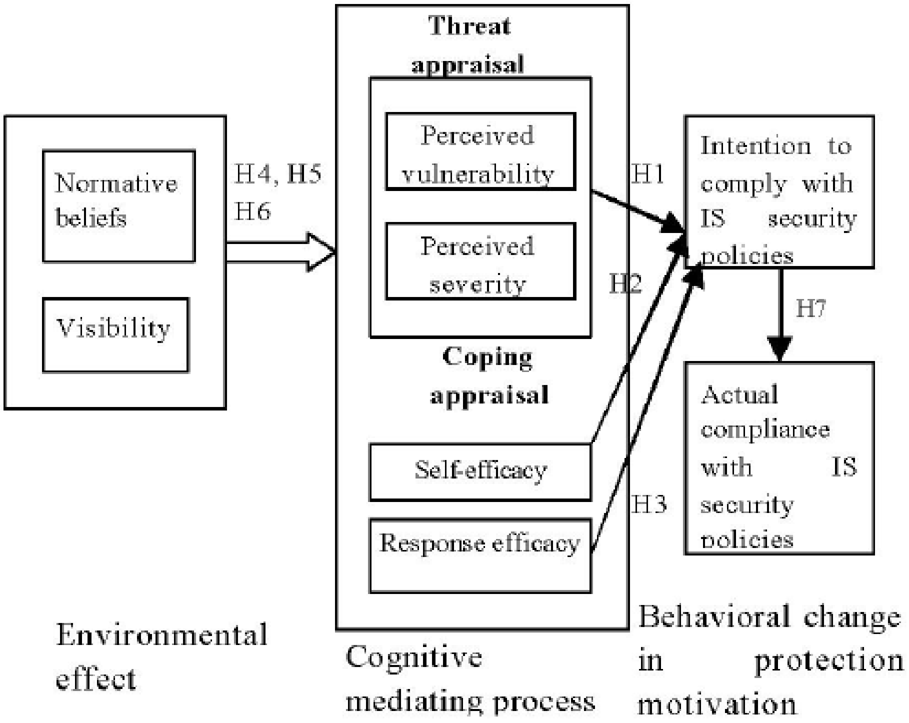
Motivational Models

Based on the above theories on motivation, researchers have examined the influence perceptions and beliefs have on ISP. These models provide statistical evidence for a direct positive relationship between an employee's perceptions and beliefs and information security policy buy-in.

Siponen, Pahnila, and Mahmood

Using Protection Motivation Theory as the basis of their research, Siponen, Pahnila, and Mahmood (2006) examined the positive effects perceptions and beliefs have on ISP buy-in. They argue that these effects may be separated into three categories: "environmental effect," "cognitive mediating process," and "behavioral change in protection motivation." The researchers argue that environmental effects (threat of punishment) lead to a cognitive mediation process (perceptions and beliefs of the threat) that motivates behavioral change (the reaction to handling the threat). They claim that this behavioral change includes intent to comply with information security policies (ISP buy-in) and, consequently, influences the actual compliance with those policies. An illustration of the model proposed to test assertions is presented in Figure 1 below (Siponen et al. 2006):

Figure 1: The research model as proposed by Siponen et al. (2006)



Source: Siponen et al. 2006, 2

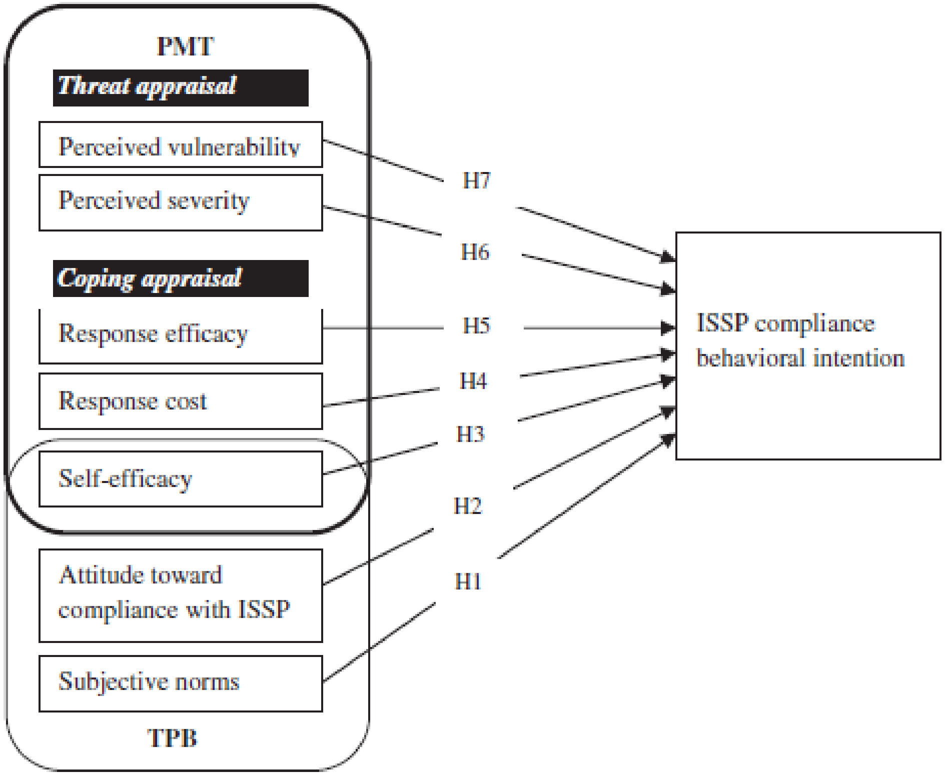
Siponen et al. (2006) validated their model through the use of a survey that was administered to five companies within the private sector. The respondents were asked to answer questions regarding the three categories mentioned above. Their responses were then gathered and analyzed for statistical significance.

From this analysis, Siponen et al.(2006) discovered that normative beliefs and visibility of the ISP and its requirements do influence an individual's threat and coping appraisals, threat and coping appraisals influence intent to comply with information security policies, and intent does significantly affect actual compliance. The authors conclude that these results "suggest that social pressure within the organization and the employees' awareness about the threats of [information systems] security have influence on the cognitive process of PMT" (Siponen et al. 2006, 4).

Ifinedo

Ifinedo (2012) incorporates both Protection Motivation Theory and the Theory of Planned Behavior, to examine how perceptions and beliefs have a direct positive influence on intent to comply with ISP. Based upon these theories, Ifinedo (2012) presents a research model by overlapping the PMT and TPB at the point of self-efficacy. Self-efficacy being an internalized belief, Ifinedo (2012) felt as though the fears associated with PMT would create internalized feelings within the individual which would ultimately affect the intentions associated with TPB. He then asserts that the combination of these fears and intentions lead to the ultimate intention of ISP buy-in. Since self-efficacy is the only common variable between the two theories, it creates a bridge to use these theories in conjunction with one another. An illustration of the model is presented in Figure 2 below (Ifinedo 2012):

Figure 2: The research model as proposed by Ifinedo (2012)



Note: ISSP represents Information System Security Policy

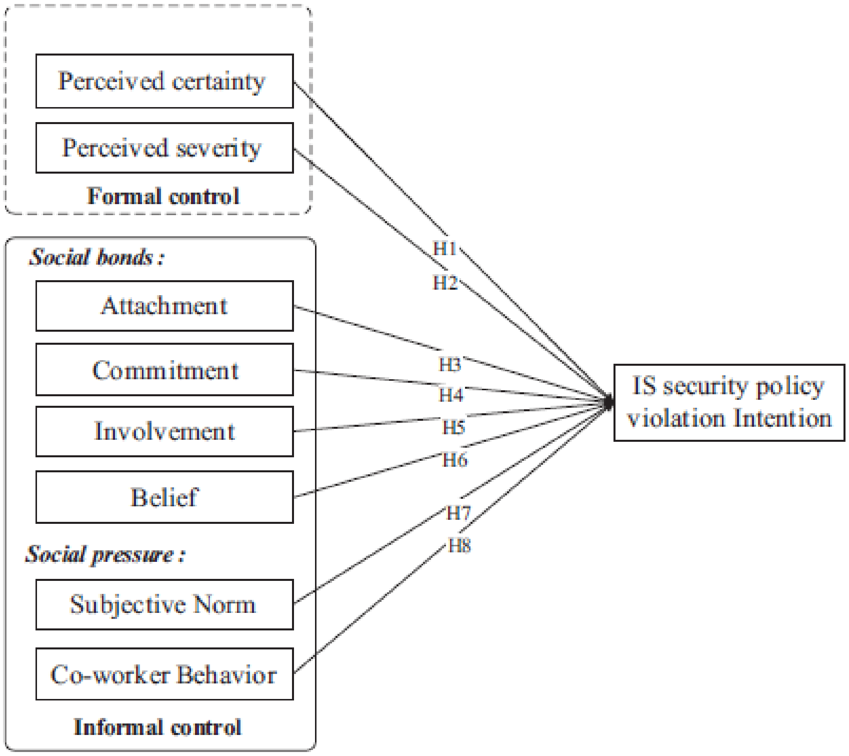
Source: Ifinedo 2012, 86

To validate his model, Ifinedo (2012) surveyed professionals of a variety of ranks and industries (both government and non-government). Resulting from this survey, Ifinedo (2012) argue that five of the seven variables are supported as positive influencers on ISP buy-in. Variables four and six, response cost and perceived severity, are rejected due to the survey suggesting that these variables have a negative effect on ISP buy-in. However, it is confirmed that subjective norms, attitude, self-efficacy, response efficacy, and perceived vulnerability have a positive effect on the intent to comply with information security policy.

Cheng, Li, Li, Holm, and Zhai

Cheng et al. (2013) took a different approach to examining ISP compliance. Rather than looking at the variables that influence compliance, Cheng et al.(2013) look into what perceptions and beliefs affect noncompliance. In doing this, two separate theoretical concepts known as General Deterrence Theory (GDT) and Social Control Theory (SCT) are utilized. GDT holds that formal controls such as “dismissal, demotion, and suspension” may be set in place by an organization to deter employees from noncompliance. SCT on the other hand suggests that there are informal controls such as peer and supervisory influence that may alter employee behavior in the realm of compliance. Figure 3 below illustrates the model developed by Cheng et al. (Cheng et al. 2013):

Figure 3: The research model as proposed by Cheng et al. 2013



Source: Cheng et al. 2013, 451

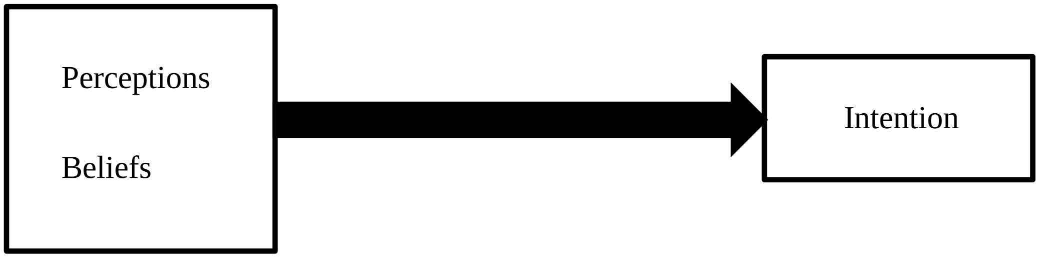
Just as with the other two models previously reviewed, Cheng et al. (2013) utilized a survey to test their model. This survey was broken into components to test the GDT and the SCT. The questions focusing on General Deterrence Theory focused on the perceived penalties associated with noncompliance. For instance, Cheng et al. (2013) asked the respondents to rate their perceptions regarding the probability of being reprimanded and the severity of that reprimand as a result of an ISP violation. The section on the Social Control Theory examined the perceptions and beliefs relating to an employee’s relationships. For example, the researchers asked the respondents to rate their beliefs regarding coworker expectations on them. The respondents were also asked to rate how committed they felt toward working with their coworkers and supervisors. The surveyed individuals were presented with four separate scenarios relating to ISP violations and asked to answer questions, such as the ones mentioned above, about how they felt regarding different aspects of the scenario presented. These surveyed individuals were of a wide range of ages, educations, experiences, and industries and all fell within the jurisdiction of at least one ISP.

In testing this model, Cheng et al. (2013) find perceived severity, attachment to job, attachment to organization, commitment, belief, and subjective norms to be significant in their negative relationship regarding an individual's intent to violate an information security policy. Also, the behavior of co-workers is found to positively impact intent for noncompliance; however, the remaining variables of attachment to supervisors, attachment to co-workers, involvement, and the perceived chance of sanctions are not found to significantly impact intent to noncomply with information security policies. Note that this model and Siponen et al.'s model contradicts Ifinedo's and shows perceived severity to be statistically significant; however, contrary to the other two models, Cheng et al. does not find perceived certainty (i.e., perceived vulnerability) to be statistically significant.

Siponen et al. (2006), Ifinedo (2012), and Cheng et al. (2013), all have different models that they tested to determine intent to comply, or not comply, with information security policies. This could pose a problem as one model may find a variable to be significant based upon a certain motivational theory while another model may find that same variable to be insignificant based upon an entirely different theory. This issue was represented within the three models by the variable of perceived severity.

This inconsistency being said, all of these models do maintain consistency in showing a direct relationship between employee perceptions and beliefs and information security policy buy-in as depicted in Figure 4 below. Within this relationship, the studies imply that perceptions and beliefs are an issue of the individual and only that individual can affect his/her intentions. However, this relationship between perceptions and beliefs and intention to comply with ISP (ISP buy-in) is all that the studies show and that is not enough. These models completely ignore the fact that leaders have motivational tools such as incentives, capacity-building, and authority that influence this relationship. They portray a simplistic approach of perceptions/beliefs equals ISP buy-in. The proposed model in the next chapter makes up for this shortcoming by asserting that perceptions/beliefs plus the moderating effect of motivational tools equals strengthened ISP buy-in.

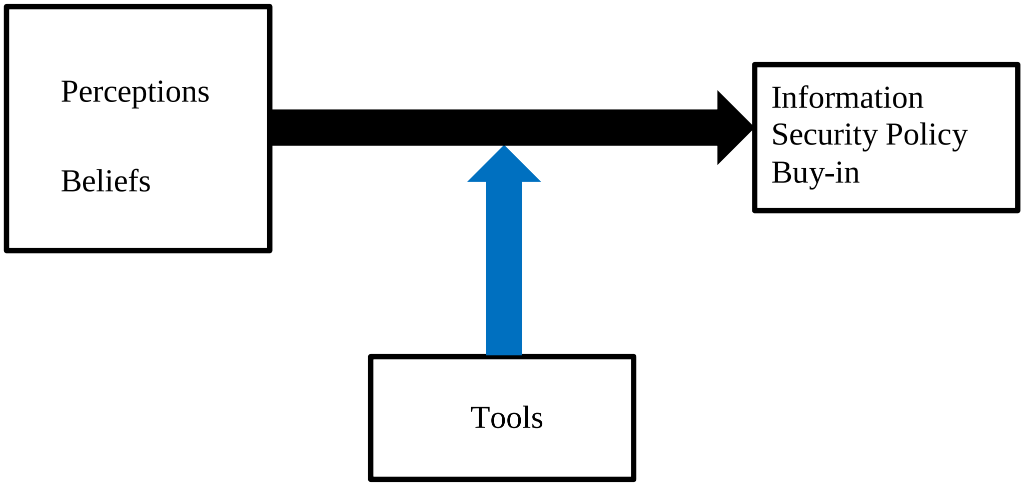
Figure 4: Basic Relationship as Depicted by Models in Literature



Chapter 3: Proposed Model

The literature reviewed in Chapter 2 outlines the effect that perceptions and beliefs have on ISP buy-in. Based on the various motivational theories, the authors of the previous models established that the intrinsic (beliefs) and extrinsic (perceptions) factors compel employees to adhere to ISP. However, what is missing is the influence leadership can have on this this relationship. The model illustrated in Figure 5 below builds upon the perceptions/beliefs that the literature shows as strong motivations for ISP buy-in and adds tools that moderate this relationship in order to strengthen ISP buy-in. This model addresses the question originally presented in Chapter 1: How can leaders motivate their employees to buy into ISP?

Figure 5: Illustration of Tools as Moderators



To illustrate this moderating effect in more detail, Table 1 below presents an example set of perceptions, beliefs, and tools. While employees hold many different perceptions and beliefs that influence ISP buy-in, those depicted within the table serve well to help explain the model from Figure 5 because these perceptions and beliefs have been shown to be strong motivators, specifically in the area of ISP buy-in. The specific tools presented below were discussed by Schneider and Ingram (1990) as being available to leaders in both federal and corporate organizations.

In reviewing Table 1 below, note a pattern on the effects the positive and negative of each tool has on the perceptions and beliefs. Given different variables and different tools, the pattern of positive tools influencing beliefs and negative tools influencing perceptions will undoubtedly change. Further discussion of these specific perceptions, beliefs, and tools, and their proposed effects on information security policy buy-in follows.

Table 1: Moderating Effects of Motivational Tools

		Incentive		**Capacity-Building**		**Authority**	
		Positive	Negative	Positive	Negative	Positive	Negative
Perceptions	Perceived Vulnerability		X		X		X
	Perceived Severity		X		X		X
Beliefs	Normative Beliefs	X		X		X	
	Self-Efficacy	X		X		X	
Note: X denotes the proposed result of increased ISP buy-in							

Perceptions/Beliefs

Perceptions and beliefs are composed of variables tested and found to be statistically significant in predicting ISP buy-in by at least one of the models discussed in Chapter 2. The perceptions of the individual are characterized by the views that individual maintains regarding compliance with the information security policy in question. The beliefs, on the other hand, fall much more closely to the core of the individual as they are the internalized feelings the individual has regarding ISP compliance. Both drive an individual’s motivation toward, or away from, ISP buy-in. Therefore, leaders must find ways to enhance their employees’ perceptions and beliefs to motivate those employees toward information security policy buy-in.

Perceptions

Perceived vulnerability refers to the perceived likelihood of an individual receiving a punishment for ISP noncompliance (Aurigemma and Panko 2012). An individual that perceives high certainty in receiving a punishment such as being fired from his/her job for violating ISP will be more inclined to buy into the ISP than an individual who does not hold such a strong perception. Perceived vulnerability is also valuable due to a discrepancy amongst the previously reviewed models in the literature. Ifinedo (2012) and Siponen et al.(2006) both found perceived vulnerability to be statistically significant in predicting ISP buy-in; however, Cheng et al. (2013) did not. This discrepancy suggests further testing of the variable for correlation with ISP buy-in.

Perceived severity, relates to perceived vulnerability in the fact that perceived severity is the individual's view of the harshness of the outcome due to the realization of a threat (Aurigemma and Panko 2012). What this means is that perceived vulnerability, as stated above, is the employee's viewed likelihood of receiving a punishment, while perceived severity is the employee's view of the extent of that punishment under the assumption that it will indeed be inflicted upon the employee. For instance, an employee may believe he/she is certain to be reprimanded for noncompliance and views the punishment to be suspension for a week rather than complete termination from employment. This threat could very well be the punishment that results from noncompliance with ISP. If an individual believes he/she will receive a severe punishment for insecure practices, he/she may be more inclined to comply with the policy and vice versa. This effect makes perceived severity relevant in the proposed model. Additionally, perceived severity is included in the model due to a discrepancy in the previously reviewed models. Out of the three models, Siponen et al. (2006) and Cheng et al. (2013) found perceived severity to be statistically significant; however, Ifinedo (2012) did not. Just as with perceived vulnerability, this discrepancy suggests that the variable should be tested further for correlation with information security policy buy-in.

Beliefs

As discussed previously, beliefs are characterized by how an individual personally feels regarding specific aspects of the information security policy, the organization, and/or themselves. Normative beliefs are the individual's feelings regarding supervisor and coworker expectations that have been placed upon the individual (Siponen et al. 2006). Normative beliefs are valuable because they relate to the individual's feelings regarding his/her environment. An individual that believes too much pressure is being placed upon his/her shoulders by coworkers and supervisors will begin to lose satisfaction in his/her work and become much more resistant to the expectations, a result that leaders should attempt to avoid. By reducing the stress that accompanies believed expectations, the employee's resistance to ISP may be reduced and his/her level of buy-in may be increased.

Self-efficacy on the other hand refers to an individual's feelings regarding his/her ability to comply with an ISP. Self-efficacy holds that an individual who believes he/she has the ability to follow an information security policy will be much more motivated to buy into the policy itself than an individual who does not maintain such a belief. This variable is included because employees who do not have confidence in their own abilities will lose their drive to even make an attempt at ISP compliance. This creates a weakness in the organization’s culture; and as was seen in the case of Target’s point of sale system, one weakness has the potential to propagate throughout the entire system. However, an employee who believes in his/her ability to comply with an ISP will buy into that policy and likewise influence help to influence his/her coworkers, resulting in a more widespread increase in ISP buy-in.

Many people act upon emotions and those emotions constitute their perceptions and beliefs which influence their decisions. The choice to buy into information security policy is exactly that, a choice. The perceptions and beliefs included in this model reflect an individual’s emotions. As has been shown by prior research, vulnerability, severity, peer pressure, and confidence in oneself influences an individual’s buy-in of an organizations ISP. These perceptions and beliefs serve as the core to an individual’s motivations; therefore, through the use of motivational tools, leaders can influence their employees toward ISP buy-in.

Tools

While difficult to alter an individual’s perceptions and beliefs, a leader can use various tools to influence the relationship between perceptions and beliefs and ISP buy-in. The tools proposed in the model are used as moderators, variables that alter the strength of the relationship between independent and dependent variables (Baron and Kenny 1986). In the context of the proposed model, the independent variables are the perceptions and beliefs while the dependent variable is information security policy buy-in. While a relationship between the independent and dependent variables has already been established, these motivational tools are meant to moderate the strength of that relationship.

The tools illustrated in Figure 5 are broad tools. For example, when looking at these tools, what kind of incentives and what kind of authority should leaders use? The answer depends on the organization and the motivation of its employees as employees will have different motivations and, therefore, not all tools will have the same effect. In some organizations, some employees view immediate recognition as a reward while others may require monetary or physical incentives. The authority may range from a verbal reprimand to a fine and/or suspension from duty. Aurigemma et al. reinforces incentives and authority as tools. These tools influence the perception of the individual in an attempt to promote compliance (Aurigemma and Panko 2012).

Other tools an organization uses will depend upon the established culture of that organization. For example, capacity-building includes learning and awareness, which refers to employees being alert of the information security risks covered by an ISP. Another part of capacity-building, training and education, assists awareness by showing employees how they may mitigate those risks while remaining policy compliant. In order to use awareness, training, and education effectively, a structured culture must be present. This culture must promote the communication between leaders and employees so that they may have knowledge of the importance of information security (Rocha et al. 2014). The effective use of these tools creates a strong influential effect on employee perceptions and beliefs which ultimately leads to ISP buy-in. The primary goal of any organization should be to utilize motivational tools in such a way as to continually push perceptions and beliefs toward ISP buy-in (Padayachee 2012). The discussion that follows includes the motivational tools the author of this thesis claims to be instrumental for leaders in enhancing the relationship between perceptions and beliefs and ISP buy-in. Each of these tools - incentives, capacity-building, and authority - is accompanied by propositions relating to that tool's moderating effects.

Incentives

Incentives are intended to get individuals to take actions they may not have taken without the incentive being in place. Incentives are utilized to help an employee overcome the hurdles to carrying out the actions required by a policy (Schneider and Ingram 1990) and to motivate that employee to buy into an ISP by altering his/her views regarding whether a benefit will result from compliance with the ISP. One example of an incentive is that of rewarding positive behavior. In rewarding positive behavior, leaders are working to reinforce the desired behavior of ISP buy-in (Eysenck 1982). This may be done through rewards such as an end-of-the-year salary bonus for ISP compliance. An employee who perceives this reward (i.e., sees that a salary bonus is being offered for ISP compliance) and believes that the organization will follow through with providing it to the employee may be more motivated toward buying into the ISP than an employee who neither perceives nor believes in the reward.

The belief is that by rewarding individuals for behavior that promotes information security compliance, the volume of secure behavior will increase within the organization. To accomplish this promotion of secure behavior, individuals must be able to see an immediate, tangible outcome from secure practices. In the example of the salary bonus, the employee must be able to see that the bonus is not an "empty promise." This mentally validates the user’s activities and helps him/her to feel positively that his/her actions are paying off (Deci 1972). By reinforcing the behavior through validation, leaders may motivate employees into believing that compliance with an ISP will result in positive outcomes.

In addition to positive incentives, leaders have the option of negative incentives to influence employee perceptions and beliefs toward ISP buy-in. One method of utilizing negative incentives (i.e., disincentives) is through the punishing of noncompliant behavior. In order for this punishment to be effective in influencing employee motivations, employees must understand what behavior has caused them to be punished. For example, within the context of information security, a method for catching and punishing noncompliance is through the use of automated systems. “Users who make poor security decisions could receive automated email notifications of their actions and the [violation of] corporate policy or safe computing practice” (West 2008, 40). The organization must then follow up with some sort of punishment such as a written reprimand or some other negative consequence.

Automated detection systems will not catch everything; therefore, another method for catching and punishing noncompliance is through anonymous peer disclosure. Organizations and federal entities often have a system in place in which employees may anonymously call a hotline to disclose policy violations they have witnessed. This hotline allows employees to feel invested in the security of the organization without the fear of potential retaliation. The organization must then follow up to confirm that the peer disclosure is valid before punitive action takes place.

The benefit of negative incentives is that they are more cost effective than positive incentives. While positive incentives are necessary to be present at all times, negative incentives are only utilized after undesired behaviors occur. By denying an individual a positive reward or punishing a behavior, that individual feels emotionally separated from his/her peers and may be more inclined to comply with organizational desires (Oliver 1980). Whether the incentive is positive or negative, one thing is for certain: incentives are an effective tool for motivating employees toward information security policy buy-in.

Four propositions reflecting this effectiveness on ISP buy-in are listed below. An example of the meaning behind these propositions may be found in the following explanation of P1. Proposition 1 illustrates the assertion that negative incentives, such as punishing noncompliant behavior, shows employees that the organization is serious regarding buy-in and will not hesitate to enforce an ISP. This disincentive increases the perceived probability of punishment (perceived vulnerability). With the relationship that the higher the perceived vulnerability, the higher the ISP buy-in already established; this increase in perception due to the dis-incentive works to strengthen the information security policy buy-in.

P1 – The relationship between perceived vulnerability and ISP buy-in is positively moderated by negative incentives

P2 – The relationship between perceived severity and ISP buy-in is positively moderated by negative incentives

P3 – The relationship between normative beliefs and ISP buy-in is positively moderated by positive incentives

P4 – The relationship between self-efficacy and ISP buy-in is positively moderated by positive incentives

Capacity-Building

Another tool is that of capacity-building, the concept of simplifying the employee's efforts to complete a task (Schneider and Ingram 1990). The underlying assumption behind this tool is that the simpler the task is to complete, the more likely it is to be accepted (Teo et al. 1999). In the context of ISP buy-in, this asserts that the easier it is for an employee to comply with the policy, the higher the chance of that employee buying into the ISP.

In order to help simplify the efforts of ISP compliance, capacity-building has many options including the reduction of costs for implementing secure policies and practices. An organization needs to present employees with simple means to accomplish secure activities. If the employee must take additional steps to be secure, he/she may be less inclined to do so depending on the difficulty and number of steps required (West 2008).

In addition to the reduction in implementation costs recommended by West (2008), Brudney and England (1983) suggest the use of a technique they call "coproduction." Coproduction is "the critical mix of activities that service agents and citizens contribute to the provision of public services" (Brudney and England 1983, 59). In other words, coproduction is the set of actions taken by professionals and citizens as a unit in order to advance the quality of the activities required by a policy. The idea is that by having professionals and citizens work together, policies will be strengthened by a diversified collection of affected individuals.

Information security policies cannot be successful unless organizations are willing to enforce them and individuals are willing to accept them. Researchers have found that

ISPs are most successful when they are carried out in a coproductive setting, rather than in an individualized setting. In other words, ISPs are most successful when cohorts of individuals/organizations work together to support the ISP implementation (Mosher 1980). Coproductive information security policy is most successful when individuals work together and build upon one another's strengths to increase information security overall (O'Toole 1987, 182).

To foster coproduction, leaders must motivate teams of their comrades and subordinates toward supporting (buying into) ISPs to achieve this higher level of success. This may be done by striving to obtain the referent power mentioned in Chapter 1 of this thesis. Leaders with referent power will have a high level of influence on their followers' perceptions and beliefs, and will be able to nurture an environment that promotes ISP buy-in amongst all individuals within the team.

Another aspect of capacity-building is the concept of increasing employee awareness. This initiative to increase awareness may be implemented in a number of ways, including through education and training seminars (West 2008) to increase employee awareness and ultimately knowledge.

Knowledge is power and employees who have knowledge regarding secure practices need to help others to become aware of security risks and of simple ways to help combat those risks. Another means of increasing awareness is through organizational leaders promoting the implementation of easily distinguishable pop-up alerts. Users often click past pop-up boxes thinking that they are not of significant importance. If the systems in place were to incorporate a set style for security alerts and have all employees know this style at a glance, the employees may be more inclined to pause for a moment and read the alert prior to dismissing it. This would help security departments to detect unsecure activities in a much more efficient manner (West 2008) as well as increase employee perceptions that their activities are indeed being monitored by others within the organization.

In order for increased awareness to be successful, employees must have the desire to learn and increase their awareness of their situations. For the highest level of success in increasing awareness, employees must be self-driven and accept the importance of the material being taught (Vandergrift 2005). Assuming this desire for increased awareness is present, it is through the education of employees that capacity-building tools may be highly successful. By educating employees in such a way as to help them understand the possible ramifications of unsecure practices, those employees may be more inclined to practice information security. They will understand the usefulness of automated pop-up alerts and report those alerts to appropriate officials. Also, educated employees may increase the awareness of security risks by helping to educate other employees, an effort that may increase the buy-in of information security policies overall.

Capacity-building works to make employees jobs easier by helping to implement ISP through methods of increased effectiveness and efficiency. Reduction of costs (automation), coproduction (teamwork), and increased awareness (knowledge) all provide easier means for employees to comply with an ISP. By reducing the efforts necessary of any one individual, an environment where employees are more inclined to buy into and accept ISP becomes more prevalent.

The four propositions listed below outline the effects of capacity-building on the relationship between perceptions and beliefs and ISP buy-in. An example explanation of these propositions may be found in P5. Proposition 5 asserts that capacity-building such as an increase in awareness of the penalties for noncompliance with an ISP positively influences the relationship with perceived severity. This is because an employee who becomes more aware of the ISP and its implications will also become more aware of the ramifications that result from noncompliance. This newfound awareness of the consequences for noncompliance increases the perceived severity of a violation in the policy. The higher the perceived severity, the higher the ISP buy-in; therefore, an increase in awareness will enhance the buy-in by increasing the level of severity perceived by the employee.

P5 – The relationship between perceived vulnerability and ISP buy-in is positively moderated by negative capacity-building

P6 – The relationship between perceived severity and ISP buy-in is positively moderated by negative capacity-building

P7 – The relationship between normative beliefs and ISP buy-in is positively moderated by positive capacity-building

P8 – The relationship between self-efficacy and ISP buy-in is positively moderated by positive capacity-building

Authority

To use authority effectively, leaders must assume one of two power structures is present in the receiving institution (the institution tasked with carrying out the policy): elitist power and pluralist power. Note that these are not the same as French and Raven's five forces of power as discussed previously. Those five forces pertain to the individual leader, while elitist and pluralist power relate to the overall organization. For instance, elitist power holds that the organization maintains a steady, structured power system.

Employees know their place and do not deviate from that structure (Bachrach and Baratz 1962). An example of this is evident within the U.S. military where rank is clearly defined and adhered to. However, under pluralist power, it is believed that the structure of the power is fluid and changes over time. This could cause the structure to range from constant change to almost no change (Bachrach and Baratz 1962).

These structures may either be set in stone by the organization (elitist power) or emerge out of the culture of that organization's employees (pluralist power). Therefore, it is imperative for leaders to determine the type of structure present in order to make effective decisions in influencing information security policy buy-in. The reason for this is that different structures create different environments for the employee. The organization's environment will affect how an employee feels toward the policy itself and ultimately affect the willingness to comply with the policy.

Authority also impacts an employee's perceptions regarding ISP compliance and, depending on its use, may have positive or negative effects. For instance, authority would likely have a negative effect if the employee feels as though his/her superiors are forcing him/her to carry out a task. Lowi (1972) discusses coercion in the context of authority as a means for influencing employee behavior by discussing elements within coercion. According to Lowi (1972), coercion is a technique available to governments in direct and indirect fashions. It is direct when the threat/punishment is placed directly upon the individual in a timely manner, such as immediately firing the employee and escorting him/her out of the office. Coercion may be indirect when the threat/punishment is placed upon the individual in a secondary manner (Lowi 1972) such as a fine placed upon the organization and the individual becomes responsible for that fine. In this manner, the use of coercion serves to increase the employee's perceptions regarding their vulnerability to a threat as well as the severity of that threat.

Coercion is not the only form of authority. For instance, a more positive form of authority is employee encouragement. Encouragement is very similar to positive incentives in the fact that it helps employees to perceive positive outcomes. However, where it differs is in its scope. For instance, encouragement often includes non-physical rewards for the employee; rather, it works to make the employee feel better about himself/herself and the work he/she does. Positive incentives, on the other hand, include elements of encouragement; but they may also include the physical aspects such as monetary rewards and display items for an employee's desk.

Leaders may use their authority within the organization's present power structure to encourage their employees and make those employees feel more positive toward an ISP. Often times, employees need to be encouraged to find satisfaction in the workplace. For instance, in an attempt to effectively encourage employees, most workplaces offer suggestion boxes; however, this fails when nothing is done to fulfill those suggestions. An active system through which employees can see their suggestions being carried out must be in place to encourage employees to become better aligned with the organization (Fairbank and Williams 2001). When employees feel they have made a significant contribution, they become invested in organizational interests. This investment could result in a desire to avoid penalties from ISP noncompliance, thus increasing information security policy buy-in.

According to Loiseau (2011), Psychologist Frederick Herzberg asserted that encouragement is an absolute factor in motivating employee behavior. Leaders may encourage employees by presenting them with reassurance such as opportunities for personal growth, increased responsibility and advancement in their work, acknowledgement for accomplishments, and recognition for their work. By encouraging employees, an organization may be able to motivate them to go above and beyond their minimum job requirements. This goes hand-in-hand with policy buy-in. If an organization is successful in encouraging its employees as they comply with policies, the employees may be more inclined to buy-into those policies.

Four propositions reflecting this influence authority has on the relationship between employee perceptions and beliefs and ISP buy-in are listed below. An example of authority as a moderator is found in the following discussion of P11. Proposition 11 states that the use of authority such as through encouragement strengthens the relationship between self-efficacy and ISP buy-in. By encouraging an employee in different ways such as showing recognition for work and giving the employee the reward of increased responsibility, a leader may increase the employee's belief that he/she has the ability to complete the tasks (self-efficacy) required by the ISP. The higher the self-efficacy, the higher the buy-in; therefore, encouragement may increase self-efficacy and thus increase ISP buy-in.

P9 – The relationship between perceived vulnerability and ISP buy-in is positively moderated by negative authority

P10 – The relationship between perceived severity and ISP buy-in is positively moderated by negative authority

P11 – The relationship between normative beliefs and ISP buy-in is positively moderated by positive authority

P12 – The relationship between self-efficacy and ISP buy-in is positively moderated by positive authority

The above tools (incentives, capacity-building, and authority) may be used separately or in combination with one another. As can be seen, the use of motivational tools is vital to the success of any information security policy. West (2008) states that tools like those mentioned above are all acceptable and have at least one thing in common: they all influence the perceptions and beliefs of the employee. The motivational tools an organization uses to influence compliance ultimately affect its employees' perceptions and beliefs of the outcomes from compliance and/or noncompliance. Whether incentives, capacity-building, authority, or a combination thereof is used will be determined by the leadership of the organization.

While there are numerous motivational tools at a leader's disposal, the ones outlined above are the most commonly used tools for motivating ISP buy-in. The use of these tools helps to increase the success of implementation and, in turn, of the policy overall. Simply believing that these motivational tools have a moderating effect on this relationship is not enough. They must be tested to confirm or deny their effects. The next chapter provides the proposed methodology for testing these propositions for significance. The proposed research methodology that follows is by no means the only methodology for testing the model proposed within this chapter; however, it is what the author of this thesis believes to be the best method at the point in time that this thesis is written.

Chapter 4: Proposed Research Methodology

In an ideal environment, testing the proposed model would be accomplished in a number of ways, including through key informant interviews (Sofaer 2002) followed by experimentation utilizing. However, it is highly unlikely that any agency and/or organization would allow for experimentation of their employees and motivational structure (i.e., leadership, incentives, teams, etc.). Therefore, this chapter discusses the proposed research methodology in the absence of experimentation and also includes the less desirable, but more likely to be permitted, option of surveys.

The first step in testing this model is to identify key informants to allow researchers to obtain highly focused data derived from the main actors that have been identified as relating most closely to the area of study (Sofaer 1999). For the proposed model, key informant interviews would allow the researcher to identify the most influential employees and utilize that influence to determine the strength of moderators such as authority and learning.

At this point, the next step to follow conduct a survey to respondents utilizing the information gathered from the key informant interviews. The type of survey recommended is known as a trend survey which is characterized by the sampling of a population of individuals over time to determine a trend in intentions ("Survey Methods" 1999). In this case, the researcher can find an organization already planning to implement a motivational tool and survey the employees of that organization prior to the tool's implementation. The researcher may then resurvey the employees after the tool has been in effect for a specified period of time to see if their intentions to comply with

ISP have changed. This is very similar to experimentation; however, in conducting the survey in this fashion, the researcher measures the moderating effect through the use of a system the organization already intended to implement. This would allow for the identification of a trend in ISP buy-in upon the implementation of a motivational tool without having to obtain special permission from the organization to alter that organization’s environment.

By utilizing the methods of key informant interviews and surveys an analysis of the effects motivational tools have on the relationship between perceptions and beliefs and information security policy buy-in may be conducted. Survey, while less stringent than experimentation, are sufficient in determining an employee’s intent to buy into information security policy. Whatever the steps utilized, the focus for testing the effects of motivational tools on the relationship between perceptions and beliefs and ISP buy-in should focus first on the employees’ intentions and then to actual behavior. Through this order of focus, researchers may be able to determine what tools would be most effective within different organizations so the researchers may then focus efforts on the actual behavioral effect of only those tools deemed most important for the particular organization in question.

Chapter 5: Conclusions

In conclusion, this thesis developed a new model for influencing information security policy buy-in. The analysis suggests that policy buy-in is a necessary aspect by organizational leadership and is influenced by factors such as motivational tools, perceptions, and beliefs. By understanding the motivations of its employees, an organization may further influence policy buy-in. Policy compliance must be accepted and enforced by leadership before employees will be willing to buy into information security policy.

While perceptions and beliefs do in fact have a direct relationship with ISP buy-in, that relationship is not enough. Leaders may use motivational tools to enhance this relationship. This thesis proposes a new model illustrating this addition of motivational tools to increase the level of information security policy buy-in within organizations, both federal and non-federal.

Limitations

This thesis examined prior studies relating to the area of ISP buy-in. However, none of these studies included the use of motivational tools to enhance the relationship between perceptions and beliefs and ISP buy-in. Therefore, this thesis proceeded to review literature on the aspect of tools to propose the effects they may have on this relationship.

This research undoubtedly has its limitations. For instance, the concept of motivating behavior is a wide and complex issue (Hu et al. 2012) as every individual is different and may require alternate forms of motivation from the forms required by other individuals. Therefore, the scope of any one piece of research is limited in nature to the factors and frameworks incorporated within that research. Additionally, each prior study that is reviewed within a piece of research may contradict other studies not included within that specific piece of research. Utilizing multiple sources has aided in the determination of which factors are the most relevant and most widely recognized in the field of information security policy buy-in.

Another limitation is lies within the scope of the thesis itself. As illustrated simply by the studies of Siponen et al. (2006), Ifinedo (2012), and Cheng et al. (2013), there are many perceptions and beliefs, even beyond these prior studies, that have not been included. Additionally, there are numerous motivational tools at the disposal of leadership. The research in this thesis provides a sample of these perceptions, beliefs, and tools to help in the understanding of their relationships with ISP buy-in.

Future Research

Future research should include the actual testing of the model proposed and should focus on both the public and private sectors as similar, but different variables, such as a focus on monetary profit versus national security, are inherent to each sector. The initial recommended target audiences are organizations that focus their efforts on information security operations such as the National Security Agency and Symantec (a private corporation that produces information security products for profit). The reason for this is that if an organization does not put any effort on information security policy, then efforts for motivating employees to do something not required of them is futile. These organizations must establish a strong base of ISP buy-in and act as the role models for the less focused organizations to follow. Additionally, future research should incorporate alternate variables from the ones discussed in the thesis to determine their effects. Some of these could be the testing of beliefs such as job importance and non-fear based perceptions. Finally, future research should disaggregate the results into similar sectors/industries, as each sector/industry may have varying rewards, behaviors, tools, beliefs, motivations, etc. This will add an additional element of precision to the analysis as the results will be reviewed at a more detailed level.

References

Ajzen, Icek. (1985). *From intentions to actions: A theory of planned behavior*. Springer Berlin Heidelberg.

Ajzen, Icek, and Beverly L. Driver. (1991). "Prediction of leisure participation from behavioral, normative, and control beliefs: An application of the theory of planned behavior." *Leisure Sciences* 13, no. 3: 185-204.

Aurigemma, Salvatore, and Raymond Panko. (2012). “A composite framework for behavioral compliance with information security policies.” *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE.

Aytes, K. and T. Connolly. (2004). “Computer and Risky Computing Practices: A Rational Choice Perspective.” *Journal of Organizational and End User Computing*, 16, 2, 22-40.

Bachrach, Peter, and Morton S. Baratz. (1962). “Two Faces of Power.” *American Political Science Review* 56:947-52.

Baron, Reuben M., and David A. Kenny. (1986). "The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations." *Journal of personality and social psychology* 51, no. 6: 1173.

Brudney, Jeffrey, and Robert E. England. (1983). “Toward a Definition of the Coproduction Concept.” *Public Administration Review* 43:55-68

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. (2010). “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.” *MIS quarterly* 34.3.

Cheng, Lijao, et al. (2013). “Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory.” *Computers & Security* 39: 447-459.

“Committee on National Security Systems.” (2014). *CNSS*. Committee on National Security Systems, Web.

CNSSI-4009: National Information Assurance (IA) Glossary. (2006). Committee on National Security Systems. CNSS.

Congress, U. S. (1988). “Computer Security Act of 1987.” *Public Law* 100-235.

Deci, Edward L. (1972). "Intrinsic motivation, extrinsic reinforcement, and inequity." *Journal of personality and social psychology* 22, no. 1: 113.

"Definitions and Meanings." (2014). *BusinessDictionary*. WebFinance, Inc. Web.

D'Innocenzio, Anne. (2014, May 5). "Target CEO Resigns Amid Fallout From Massive Data Breach." *The Huffington Post*. TheHuffingtonPost.com. Web.

DoD Instruction 8500.2: Information Assurance (IA) Implementation. (2003, Feb 6). Department of Defense.

DoD 5400.11-R: Department of Defense Privacy Program. (2007, May 14). Department of Defense.

English Definitions. (2014). *Cambridge Dictionaries Online*. Cambridge University Press. Web.

Eysenck, Michael W. (1982). "Incentives and Motivation." In *Attention and Arousal*, pp. 67-68. Springer Berlin Heidelberg.

Fairbank, James F., and Scott David Williams. (2001). "Motivating creativity and enhancing innovation through employee suggestion system technology." *Creativity and Innovation Management* 10, no. 2: 68-74.

"Federal Information Security Management Act (FISMA) Implementation Project." (2014, Apr. 1). *NIST Computer Security Division*. National Institute of Standards and Technology, Web.

French, J. and B. Raven. (1959). *The bases of social power*. D. Cartwright and A. Zander. Group dynamics. New York: Harper & Row. Print.

Harpine, Elaine Clanton. (2008). "Motivation: Intrinsic vs. Extrinsic." *Group Interventions in Schools: Promoting Mental Health for At-Risk Children and Youth*: 19-26.

Herath, Tejaswini, and H. Raghav Rao. (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." *European Journal of Information Systems* 18, no. 2: 106-125.

Higgins, Huong Ngo. (1999). "Corporate system security: towards an integrated management approach." *Information Management & Computer Security* 7, no. 5: 217-222.

Hinde, Stephen. (2002, Aug 1). “Security Surveys Spring Crop.” *Computers and Security* 21.4: 310-21. *Security Surveys Spring Crop*. Science Direct. Web.

Hirschi, Travis. (1986). "On the compatibility of rational choice and social control theories of crime." *The reasoning criminal: Rational choice perspectives on offending*: 105-118.

Hu, Qing, et al. (2012). “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture.” *Decision Sciences* 43.4: 615-660.

IBM Security Services Cyber Security Intelligence Index. (2013). Rep. Somers, NY: IBM Global Technology Services.

Ifinedo, Princely. (2012). “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.” *Computers & Security* 31.1: 83-95.

"Information Security Policy." (2006). *Information Security Policy*. University of Pitsburgh.

Junger, Marianne, and Ineke Haen Marshall. (1997). "The interethnic generalizability of social control theory: An empirical test." *Journal of research in crime and delinquency* 34, no. 1: 79-112.

King, Guy. (2000). "Best Security Practices: An Overview." Computer Sciences Corporation. NIST. Web: 2

Lindner, James R. (1998). "Understanding employee motivation." *Journal of extension* 36, no. 3: 1-8.

Loiseau, Julio W. (2011, Sept.). “Herzberg's Theory of Motivation.” *Academia.edu*. N.p. Web.

Lowi, Theodore J. (1972). “Four Systems of Policy, Politics, and Choice.” *Public Administration Review* 11:298-310

Maslow, Abraham Harold. "A theory of human motivation." *Psychological review* 50, no. 4 (1943): 370.

McCumber, John. (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*. Boca Raton, FL: Auerbach Publications.

Mosher, Frederick C. (1980). “The Changing Responsibilities and Tactics of the Federal Government.” *Public Administration Review* 40:541-48

National Security Agency. (2014, Feb 10). “Congressional Notification - Resignation of NSA Employee - Information Memorandum.” Letter to Staff Director and Minority Staff Director, House Committee on the Judiciary. MS. Fort George G. Meade, Maryland.

Norman, Paul, Henk Boer, and Erwin R. Seydel. (2005). "Protection motivation theory.": 81-126.

Oliver, Pamela. (1980). "Rewards and punishments as selective incentives for collective action: theoretical investigations." *American journal of sociology*: 1356-1375.

O’Toole, Laurence J. (1987). “Policy Recommendations for Multi-Actor Implementation: An Assessment of the Field.” *Journal of Public Policy* 6:191-210

Padayachee, Keshnee. (2012). “Taxonomy of compliant information security behavior.” *Computers & Security* 31.5: 673-680.

“Regulatory Compliance Demystified: An Introduction to Compliance for Developers.” (2006, Mar.) *Regulatory Compliance Demystified*. Security Innovation, Inc. Web.

Rocha, Flores, Waldo, Egil Antonsen, and Mathias Ekstedt. (2014). “Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture.” *Computers & Security* 43: 90-110.

Rippetoe, Patricia A., and Ronald W. Rogers. (1987). "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat." *Journal of personality and social psychology* 52, no. 3: 596.

Ryan, Richard M., and Edward L. Deci. (2000). "Intrinsic and extrinsic motivations: Classic definitions and new directions." *Contemporary educational psychology* 25, no. 1: 54-67

Schneider, Anne, and Helen Ingram. (1990). “Behavioral Assumptions of Policy Tools.” *The Journal of Politics* 52.02: 510.

Siponen, Mikko, Seppo Pahnila, and Adam Mahmood. (2006). “Factors Influencing Protection Motivation and IS Security Policy Compliance.” *IEEE Xplore*. Innovations in Information Technology. Web.

Sofaer, Shoshanna. (1999). "Qualitative methods: what are they and why use them?." *Health services research* 34, no. 5 Pt 2: 1101.

Sofaer, Shoshanna. (2002). "Qualitative research methods." *International Journal for Quality in Health Care* 14, no. 4: 329-336.

"Survey Methods." (1999). *Survey Methods*. University of Texas. Web.

Teo, Thompson SH, Vivien KG Lim, and Raye YC Lai. (1999). "Intrinsic and extrinsic motivation in Internet usage." *Omega* 27, no. 1: 25-37.

Thornton, Dorothy, Neil A. Gunningham, and Robert A. Kagan. (2005). "General deterrence and corporate environmental behavior*." *Law & Policy* 27, no. 2: 262-288.

Usher, Alexandra, and Nancy Kober. (2012). "1. What Is Motivation and Why Does It Matter?." *Center on Education Policy*.

Vandergrift, Larry. (2005). "Relationships among motivation orientations, metacognitive awareness and proficiency in L2 listening." *Applied linguistics* 26, no. 1: 70-89.

Von Neumann, John, and Oskar Morgenstern. (2007). *Theory of Games and Economic Behavior (60th Anniversary Commemorative Edition)*. Princeton university press.

West, Ryan. (2008, Apr. 1). “The Psychology of Security.” *The Psychology of Security*. Association for Computing Machinery. Web.

Whitman, Michael E. (2008). "Security Policy." *Policy, Processes and Practices*): 123.

Williams, K. R., and R. Hawkins. (1986). “Perceptual research on general deterrence: A critical review.” *Law and Society Review*, 545-572.

18 U.S. C. § 37-798 (2011). U.S. Government Printing Office.

2014 Information Security Breaches Survey. (2014). Rep. London: Department for Business, Innovation and Skills.

Appendix A

Exhibit 1: Publications Developed Under the FISMA Implementation Project

Publication	Title
Federal Information Processing Standard (FIPS) 199	Standards for Security Categorization of Federal Information and Information Systems
Federal Information Processing Standard (FIPS) 200	Minimum Security Requirements for Federal Information and Information Systems
NIST Special Publication (SP) 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems
NIST Special Publication (SP) 800-39	Managing Information Security Risk
NIST Special Publication (SP) 800-53	Recommended Security Controls for Federal Information Systems and Organizations
NIST Special Publication (SP) 800-53A	Guide for Assessing the Security Controls in Federal Information Systems and Organizations
NIST Special Publication (SP) 800-59	Guideline for Identifying an Information System as a National Security System
NIST Special Publication (SP) 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories

Exhibit 2: Additional Legislation Relevant to Information Security Policy

Act	Applies to
Sarbanes-Oxley	Privacy and integrity of financial data in publicly traded corporations.
HIPAA	Confidentiality, integrity, and availability of health care information.
PCI	Confidentiality of credit card information stored and used by merchants.
GLBA	Confidentiality and integrity of personal financial information stored by financial institutions.
SB 1386	Confidentiality of customers' personal information stored by any organization that does business in the state of California.

Source: "Regulatory Compliance Demystified" 2006