Walden University

COLLEGE OF MANAGEMENT AND TECHNOLOGY

This is to certify that the doctoral dissertation by

Gregory Edwards

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Steven Tippins, Committee Chairperson,
Applied Management and Decision Sciences Faculty

Dr. Raghu Korrapati, Committee Member,
Applied Management and Decision Sciences Faculty

Dr. Walter McCollum, University Reviewer
Applied Management and Decision Sciences Faculty

Chief Academic Officer

David Clinefelter, Ph.D.

Walden University
2011

Abstract

Federal Government Information Systems Security Management and Governance are Pacing Factors for Innovation

by

Gregory Edwards

M.S., Webster University, 1989

B.S., Park University, 1982 & 2001

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

February 2011

Abstract

Security incidents resulting from human error or subversive actions have caused major financial losses, reduced business productivity or efficiency, and threatened national security. Some research suggests that information system security frameworks lack emphasis on human involvement as a significant cause for security problems in a rapidly changing information technology environment. The purpose of this case study was to discover central themes that can shape the future for information security management, governance, and laws in the federal government. The theoretical foundation for the study was derived from McGregor's X and Y theory principles. The research questions focused on ranking ways to synchronize information system security management, governance, and legal actions to form the most efficacious model possible. A survey that contained 40 core themes drawn from empirical research in the information system security field was administered to a purposive sample of 100 federal government managers to assess their level of agreement with each practice. Categorical analysis of survey data were used to compare patterns of responses to theoretical principles in order to propose practices and controls needed to motivate employees to achieve organizational goals and objectives. The categorized results highlighted 13 principles that addressed strengthening strategic planning, policy development, human management, training and education, and standardization now and in the future. This study contributes to positive social change by informing methods of human resource management that can increase the efficacy and reliability of security performance within key information systems used to ensure the safety of individuals and organizations against a variety of internal and external threats.

Federal Government Information Systems Security Management and Governance are Pacing Factors for Innovation

by

Gregory Edwards

M.S., Webster University, 1989

B.S., Park University, 1982 & 2001

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Information Systems Management

Walden University

February 2011

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Dedication

To the everlasting memory of my late mother, Ruby Lee, and wife and mother of our children, Suk Ja, for their love and support.

Acknowledgments

Dr. Steven Tippins has been a wonderful mentor and leader throughout this entire learning process. Dr. Raghu Korrapati's support through the proposal and oral defense processes is dearly appreciated. A special thanks to Dr. Gary Burkholder for the time he took to give me theoretical framework guidance during a residency intensive dissertation review course.

I would like to acknowledge my sons, Corey and Brian, for their love and support even though my studies often kept me from spending more time with them as they completed college.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

The pervasiveness of information systems throughout organizations has provided many efficiency and productivity benefits but also caused an enormous security burden. Baker and Wallace (2007) suggested that the intrinsic value of information technology (IT) systems dwarfs the mission critical functions they support. Despite this intrinsic value, wide spread use and significance of information systems to business operations, managers continue to struggle in finding ways to ensure they are putting the correct security controls in place. Baker and Wallace concluded that the overall process is an extremely difficult balancing act to find the right mixture of security controls that minimize risk but allow for continued innovation. Conner, Noonan, and Holleyman (2003) suggested that the elusive search for a proper fit between information system security controls with management and governance principles has become the pacing factor for innovation.

In order to improve efficiency while minimizing security risks Baker and Wallace (2007) proposed a detailed analysis of current information security management practices. The authors believed a basic set of controls already exist to protect the confidentiality, integrity, and availability of IT business functions. For example, many products are readily available to offer management controls for information services, processes, policies, human resource management, and federal legislation. Although these programs are available, managers are still perplexed. Baker and Wallace explained that formal information security management programs are needed to determine what specific type and degree of controls are required. There are no one size fits all solutions. For

example, the decision process must consider the internal and external customer base so confidential information is protected and releasable information shared with customers. Nonetheless, the expense of implementing and maintaining these controls is driving managers to only seek the most appropriate or minimum set of controls for the situation.

In the past, the most prevalent security approach was to use the latest technological innovations to lock down networks and create a security perimeter. Alfredo (2008) described how network intrusion devices and firewalls were being used to offer security protection through sophisticated algorithms and automated rules based access. This approach proved unrealistic due to information sharing requirements so a more holistic management methodology is the new quest. Baker and Wallace (2007) supported how the National Institute of Standards and technology (NIST) separated the various security controls into three primary categories: technical, operational, and management. Technical refers to the products and processes, operational controls are access, backups and environmental considerations. Management controls are usage policies, training programs, and contingency plans. This approach seemed to offer more flexibility while still providing adequate degrees of security in categories.

Deloitte and Touche's 2005 global security survey noted that 83 % of the respondents believed their systems had been victimized that year (p. 14). The attacks came from both inside and outside and were wide spread so compliance management required input from a combination of both technical and security solution sources. Despite the comprehensive nature of controls in the federal government's information security management system, the results were mixed. Seventeen percent felt the

government's security driven approach was effective, but the respondents believed the rules did not improve the organization's security position or reduce data protection risks. Thirty-seven percent felt the policies were a move in the right direction to provide sustained solutions. In Deloitte and Touche's 2007 global security survey, 91 % of the participants were concerned about employee security weaknesses and 79 % cite the human factor as the root cause of information security failures.

There are a number of security challenges to business operations, so agencies must be prepared for changes in threats and responses. Sixty-three percent of the surveyed people cite lack of employee awareness and training as the major issue that causes vulnerabilities (Deloitte & Touche, 2007). Risk management is therefore a major concern for most executives and why they allocate resources to address security issues. Nonetheless, Deloitte and Touche's 2007 survey results reported that 32 % of their respondents reduced their information security investments. In contrast to 2005, legislation, regulations, and lawsuits led to increased security spending on compliance and technology solutions and this trend was expected to continue (Deloitte &Touche, 2007). The survey research results also indicated that security training was vital because human performance, in terms of ability, motivation, and environment, must be managed. The survey respondents also expressed that only 65 % of their organizations had trained their employees to identify and report suspicious activity. As indicated by the Deloitte and Touche (2005) and Deloitte and Touche (2007) surveys, various types of training are being used; however, these programs will not be effective until people are motivated to follow security guidelines, policies, and procedures.

Although there is widespread agreement that several useful frameworks have been developed, consensus is that frameworks or models that offer the correct fit for management and governance are lacking. The information security issue was seen as a technical problem (Brown & Grant, 2005). An example of a correct fit is finding a security access control like password and login features that are difficult to break but easy for employees to remember and use. For example, single sign on applications are solutions developed to prevent users from having to remember multiple passwords (Department of Commerce, 2006a). Baker and Wallace (2007) believed it was the initial technical only focus on solving IT security problems that caused this management and technical solution chasm. In opposition to a technical only solution set, the Federal Information Security Management Act (FISMA) served as a foundational information security governance document that has directed management actions to improve the effectiveness of information security programs in the federal government (Nowell, 2007). Nowell's analysis suggested the structural guidance, assignment of responsibility approach, oversight agency appointments, broad coordination system, and audit control processes seem to be excellent framework lessons for other organizational programs. In addition to the federal government research and policies, the commercial sector is also engaged in discussions about management and governance solutions (Volonino, Gessner, & Kermis, 2004).

Baird (2002) explained that the debate about global governance is essentially about participation, accountability, and transparency (p. 20). Effective IT security implementation is a matter of enlightened organizational self-interest where a company

seeks to protect its own information and that entrusted to it by customers, suppliers, or other partners (Conner, Noonan, & Holleyman, 2003, p. 2). The new economic and geopolitical environment stresses the need for regulation and governance to achieve and maintain the right balance between open, networked systems, and security of closed environments. If nothing more than providing the forum for debate and discussion, the role of the government is unique as a mediator and enforcer. The road ahead is one that demands greater accountability and transparency (Baird, 2002).

As the number of Internet users around the world continues to grow, governing institutions will be expected to step in and protect people from harm as innovation is embraced. The proper application of information system security controls is a constant challenge for managers. Conner, Noonan, and Holleyman (2003) suggested a holistic management approach is required that includes technical, operational, and management solutions. It appears that managers still have not fully grasped the necessity to balance the technical and management controls to achieve optimum effectiveness at reasonable costs. As evidenced by Deloitte and Touche's survey 2005 and 2007 results, training and education programs are also lacking so the risks remain high for attacks from inside or outside the environment. The Department of Commerce implemented a rigorous and detailed security control program for the federal government and this is seen as a move in the right direction; however, the latest Government Accountability Office (GAO) report on cyber security expressed the need for increased focus on implementing controls to prevent security risks (GAO, 2009). The report indicated that pervasive attacks are taking advantage of security gaps that could be protected if controls were implemented more

effectively. Baker and Wallace (2007) revealed that people remain the weakest link so a comprehensive information security management and governance program is considered the best risk management option to gain optimum efficiency and effectiveness. The literature review in chapter 2 will delve deeper into management and behavior theory, federal information security management act principles, and governance principles.

Statement of the Problem

The research problem addressed in this study is the failure of information systems security models and frameworks to focus on management and governance solutions. A gap in the literature exists in terms of identifying key management and governance themes which can serve as elements of a more effective governance model. Increased attention to the human elemental causes for security problems in the rapidly changing information technology environment is asserted. Research has been weighted toward designing and implementing technical solutions to solve the problems (Baker & Wallace, 2007). Meanwhile, the employee behavioral and social problems stemming from these technical solutions are not being addressed.

The SANS Institute (2006) indicated predictions are for more attacks on information systems that will drive the need for increased governance to moderate the associated risks. The pervasiveness of information systems throughout organizations provided efficiency benefits; however, security incidents caused by these systems continue to double each year and increase exponentially as the number of networks increase (SANS Institute, 2006). The government's efforts to sponsor research, lead focus groups, and invest in technology have been noteworthy; but, information security remains

a massive problem that is damaging government and business operations on a global scale (SANS Institute, 2006). According to the GAO (2009), 20 of 24 major agencies indicated that inadequate information system controls over financial systems and information was a significant deficiency or a material weakness for financial statement reporting (p. 7). It is essential that managers gain an increased understanding of the key issues so the root cause of security vulnerabilities can be remediated.

Background of the Problem

Chung (2007) explained that the paradigm shifted from employee centric to knowledge based information societies. This shift has resulted in the emergence of new social norms, ethical values, and cultural trends. He went on to explain that personal blogs, wikis, and websites are common place methods used to share memories and express ideas on the public Internet. Chung asserted that trust in cyberspace has become a major social issue as people are losing their right to choose and operate in a safe and secure environment. Trust and privacy issues will continue to emerge as more and more innovations are embraced by society (Chung, 2007). Chung also stated that these innovations support social activism that builds increases in capital that lead to building closer relationships around the world. Society will demand that these trust and privacy issues be addressed (Chung, 2007).

Legal implications are also concerns in response to financial fraud and related audit issues. Chief Executive Officers (CEOs) must rely on their internal audit and information technology departments to comply with the various mandates (Lobree, 2002). The individual remains the weakest link in the information security chain but

receives less focus. Little is being done to understand the cause of human induced information security problems (Mathiasen, 2008). Information security problems are impacting society in ways never imagined and leave exploitation vulnerabilities. Baird (2002) stated that relying on markets and self policing has failed to adequately address the important interests of Internet users such as privacy protection, security, and access to diverse content (p.15). There is a need to find management and governance principles that can be used to continue shaping the information security landscape to embrace innovation and reduce risks posed by employees.

The federal information security management act (FISMA) of 2002 was enacted into law to provide a comprehensive framework to improve the effectiveness of information security management in the federal government. The act recognized the complex nature of security and the importance of including coordination requirements with civilian, national security, and law enforcement agencies. The act was structured to provide minimum controls, improved oversight, use of commercial products, and delegation of specific management responsibilities to individual agency leaders. In the broadest sense, the act was focused on ensuring integrity, confidentiality, and availability of information security services (FISMA, 2002).

Chung (2007) introduced the notion that under the mantra of information security, protection of privacy and basic human rights there is a force of anonymity in cyberspace that must be addressed. Leaders struggle to address willful and malicious acts that have been conducted to defame innocent people but avoid applying severe restrictions that infringe on basic societal rights and freedoms. Chung believed new frameworks and ideas

offered through research will be helpful in developing assertions that can help inform governance of the impacts of IT innovations on society. If nothing more than achieving a level of trust, security and privacy protections are important considerations that are affecting societal structures.

Legal issues in information technology security expressed by Volonino, Gessner, and Kermis (2004) indicated that this massive, zero tolerance legislation created challenges that required fast, accurate and verifiable information tools be developed and integrated. Companies needed to improve information quality to insure transparency, accuracy, timeliness, and reliability. Security had to be strengthened to distinguish authorized suppliers, employees, and management levels so proper access privileges could be issued. The security features had to be monitored and alerts established to notify proper authorities when unauthorized actions occurred. Lobree (2002) saw it as unfortunate that legislation came as a result of corruptness, security industry cries for rules, regulations and standardization, and the general community's plea to the government to regulate electronic commerce. Many states have also enacted laws that impact a corporation's bottom line if they are compromised. Examples of these laws include employee information privacy controls, client privacy controls, and patient and criminal records controls. Based upon the severity of resultant security problems, it appears that many of these management and technical controls were instituted without sufficient employee understanding and consideration (Lobree, 2002).

Void regulation, the individual businesses are not motivated to solve these problems holistically, because real solutions would reduce business opportunities that

provide sustaining revenue (Volonino et al, 2004). Volonino et al. stated that the standards introduced in the Federal Information Security Management Act legislation are a step in the right direction; however, they are mostly suggestions to industry instead of mandates. Volonino et al. also suggested it may be time to mandate a level of information security compliance, through standards, so the threats introduced from information technology products can be better managed. Just like the financial corruptness, information security corruptness is rampart and needs stronger governance to prevent exploitation of human good within society (Volonino et al., 2004).

The bottom line in achieving organizational goals is good leadership and management. Landell-Mills (2003) indicated that modern leadership approaches must be multidisciplinary so everyone's interests are considered and balanced in policy descriptions. As the security controls are selected there must be analysis applied in selecting specific controls to ensure proportionality. In order to have effective security throughout, managers must integrate security with overall policies. Landell-Mills saw the key components of good governance as "good public sector management with accountability in public institutions, transparent policy-making and implementation, clarity, stability and fairness in the rule of law, and openness to the participation of affected citizens" (p. 357).

Purpose of the Study

I looked to foster social change by discovering ways management and governance practices in the federal government could be improved in response to information technology security challenges. The contributions from existing federal

legislation were reviewed to gauge their effectiveness and learn about research conducted to gather information which might explain why current governance practices were not more effective. This information was synthesized to reveal the common challenges society faces and outline ideas for a new management paradigm that will help reduce negative perceptions of change. The relevance of past theoretical management principles was discussed in context with today's information security management challenges. The social impacts resulting from the need for improved information security management were analyzed to discover central research opinions and recommendations. The need to comprehensively address information security management and governance as a dire sociological governance issue was explored.

Theoretical or Conceptual Support for the Study

The relevance of past theoretical management principles was discussed in context of today's information security management challenges. McGregor's (1960) theory X and theory Y were used as the basic conceptual support for the study. An outline for each of the theory's posits for employees is described in figure 1. Theory X assumes employees are inherently lazy and will avoid work if they can and they inherently dislike work. The theory suggests that management believes the workers need to be closely supervised and a comprehensive system of control must be developed to guide their work. It further states that a narrow span of control is required so a hierarchical structure is necessary. Employees show very little ambition and must be enticed by some type of incentive programs or they will avoid responsibility. In response to this type of behavior, theory X managers rely on

coercion or threats to get employees to comply with rules or policies. A downfall of this type of managerial response can lead to mistrust and an unduly restrictive environment.

In contrast, theory Y assumes employees are ambitious; self motivated, and have self control. The employees are believed to enjoy the mental and physical aspects of their jobs (McGregor, 1960). McGregor also stated that workers are problem solvers who feel free to be creative; however, their talents are often not used properly. Theory Y managers believe employees will follow the objectives of the organization by seeking out and accepting responsibility (McGregor, 1960). Under the right conditions and circumstances, theory Y workers want to do well at work and the satisfaction of doing well is a strong motivator. McGregor (1960) believed that managers should look to apply the theory that is required for their situation and feel free to change between X and Y as appropriate.

Theory X – Posits: Employees	Theory Y – Posits: Employees
Are inherently lazy	Are ambitious and self-motivated
Inherently dislike and will avoid work	Enjoy mental and physical aspects of work
Must be closely supervised	Minimal supervision; self motivated
Comprehensive systems of controls	Freely follow established goals
Force managers rely on coercion to ensure compliance with rules or policies	Seek out and accept responsibility; motivated by satisfaction of doing well
Mistrust management and thus require an unduly restrictive environment	Trust management and perform in an open and free environment

Figure 1. Theory X & Y employee characteristics

McGregor (1960) suggested that management of the past and future is still about control, authority, and motivation of people to achieve organizational objectives or goals. The principles of theory X and Y expressed by McGregor still have applicability in today's knowledge working environment. Striving to achieve balance between the needs of the people and organization remain central challenges. Instead of focusing specifically on controls, theorists suggested a slight shift to performance measures. The modern day knowledge worker is more a theory Y person and is eager to work toward accomplishing organizational goals. It is important to seek a balance between the needs of the organization and the knowledge worker for the organization to perform effectively.

Fayol (1987) suggested there are no known formulas for success in management; however, developed theories and principles should be used to inform and guide decisions. In fact, the past theories should help in devising new approaches and solutions to management challenges. Sociological thoughts of Weber (1962) discussed interpretative understanding of human behaviors. The various interpretations or observations are used to try and explain why certain behavioral responses occur. Weber referred to the match between a behavior and response as an ideal type, but accepted there are no sure methods for knowing outcomes based on inputs when it comes to managerial theory.

Assumptions

1. Department of Defense was a good target population to sample for information systems security and governance ideas.

2. The National Defense University student population was a representative sample of the department of defense population.

3. Sufficient literary research material existed to be able to gather meaningful and well founded governance themes.

4. Managerial and behavioral theorist's principles offered insights into the development of sound information systems security governance principles.

5. The Federal Information Security Management Act (FISMA) of 2002 was founding legislation that has broad acceptance and offered a good governance model for the federal government.

6. Information systems security governance was important to protect society and support innovation.

7. Objectivity was used in analyzing and selecting the seminal themes for the literature.

Scope and Delimitations

The study included the class of 2010 permanent resident students attending the Industrial College of the Armed Forces (ICAF). The number of students was projected to be 150. The students were senior federal government managers from various departments and agencies. I focused on uncovering the ideas and thoughts of the students on key information systems security governance themes or principles. The duration of the study was 1 month. A survey questionnaire was given and responses requested in 2 weeks. An additional 2 week extension was given to allow time for more responses.

The study was limited in breadth and depth by focusing on FISMA of 2002 as founding legislation, preselected scholarly literature, specific management and behavioral theories, and a survey. The case study does not include quantitative analysis methods that seek to identify and compare independent and dependent variables. The intent of the study was to uncover and validate the synthesized themes, not to conduct comparative analysis.

Limitations

Due to the qualitative research approach, findings could not be extended to the larger federal government population with any degree of certainty. The themes that were uncovered from the research could not be generalized to the population of the entire federal government and are restricted to views expressed by senior managers attending the school. The research conclusions did not provide definitive conclusions, but offered solid research information upon which decisions can be made.

Respondents may have misunderstood some of the questions or had personal biases or experiences that influenced their responses; so, a preestablished set of questions were prepared with a limited number of response categories (Leedy & Ormrod, 2005). All respondents received the same set of questions in the same order and sequence. Each question was framed with minimum flexibility in responses in order to reduce potential misunderstanding.

Since the target population was federal government managers who were students, their views may have been altered by the thoughts of the institution, professors, and recent material read on the subject. Although these influences are

natural, the timing of introducing the survey based on the student's current classes was considered. The survey was given during a time the class was not specifically studying information security issues.

Definitions of Terms

Availability: Ensuring timely and reliable access to and use of information (FISMA, 2002).

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (FISMA, 2002).

Domain Name System (DNS): Hierarchical naming system for computers, services, or resources connected to the Internet or a private network (Malcolm, 2008).

Firewall: A gateway that limits access between networks in accordance with local security policy (NIST, 2006).

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 (FISMA, 2002).

Integrity: Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity (FISMA, 2002).

Internet Corporation for Assigned Names and Numbers (ICANN): A not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. To reach another person on the

Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world (ICANN, 2009).

Management Controls: The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security (FISMA, 2002).

Network Intrusion Device: Devices which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment (NIST, 2006).

Rules-based Access: A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access (NIST, 2006).

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (FIPS 199, 2004).

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (CNSS Instruction 4009, 2003).

WHOIS: System or application that is widely used for querying a database to determine the registrant or assignee of Internet resources, such as a domain name or IP address (Malcolm, 2008).

Research Questions

The three research questions were chosen to narrow the information systems security topic so it could be broken into manageable parts. After conducting research of existing literature the focus areas fell into three primary areas. In the first area, FISMA was the founding legislation that guided efforts to improve information security management as early as 1996. Much of the research literature discussed different managerial frameworks and theories that should be considered as tools to prevent security problems in organizations. Also, the research had an organizational and behavioral management focus.

More recent literary research mentioned the need for stronger governance models, frameworks, and principles to moderate security problems (Baker, 2002). Governance was a key theme that was spurred in response to security violations that affected financial and personal information. The research questions were, as recommended by Singleton and Straits (2005), derived from the state of current scientific knowledge.

1. How can management practices be improved in the federal government sector of society to respond to current and emerging information technology (IT) security issues?

2. How has the Federal Information Security Management Act (FISMA) contributed to improving IT security governance and management in the federal government?

3. Why are IT security governance practices not more effective in responding to current and emerging IT security issues?

Following the guidance expressed by Leedy and Ormrod (2005), the three research questions were designed as triangulation points from which the problem could be explored. The questions also served as check points against which to test the research findings that would be revealed. Each question addresses three prime areas that evolved from the research: FISMA contributions to improved security, best management practices, and leading governance strategies. After researching these three areas the themes were refined, organized, and integrated to become survey questions. The survey questions became the instrumentation in which senior manager's views were collected and analyzed during the data analysis phase.

Significance of the Study

The behavior of individuals, whether at the office or home, has continuously been cited as the prime causes of information security problems. As more innovations are introduced into the market space, managers must learn how to affect behavior that respects information security principles the same as one obeys home security, school and traffic rules within the many cultures that comprise society (Conner, Noonan & Holleyman, 2003). Conner et al. also believed that as the individual is highlighted as an essential management element of information systems, security policies and

governance, social changes will encounter less friction. A better understanding of the triggers of change, staff and management relationships, knowledge worker motivations, and affects of controls on individuals will help foster a healthy social change environment where innovation can thrive (Conner, Noonan & Holleyman, 2003).

The significance of this information security management research is discovering how to integrate theories of prominent human management researchers with information security management literary research, and governance principles. Central ideas or themes that were noted as challenges, suggestions, and general research observations were extracted and analyzed. The synthesis of these research ideas can help guide future research in this area and provide insight in developing future governance policies or legislation to enhance information security without undue restrictions to innovation. Focus on the human management aspects of ensuring governing information security controls are properly implemented and followed could also be explored.

The management, behavioral, and organizational principles developed by theorists like Drucker (2008), McGregor (1960), Fayol (1987), and Weber (1962) can be helpful in selecting information security governance controls. Working to achieve balance between the needs of people and organizations was a challenge many decades ago and continues to plague managers in today's information age society. Changes in staff and line management relationships is an example of how past and present management principles are aligning in response to information security concerns. The individual worker has become as powerful an element in the organizational structure as staff managers (McGregor, 1960). Consequently, top down guidance and direction is not as effective as

it once was in organizations. Information sharing for innovation is another factor that drives today's information organizations. Mintzberg (1989) explained how past managers created information domains to share information with partners and protect it from others. This is an example of how controls were used in different forms to deal with diverse information sharing needs.

Managers still have not fully grasped the necessity to balance the technical and management controls to achieve optimum effectiveness at reasonable costs. Therefore, this study helps inform training and education programs so the risks can be reduced from attacks inside or outside the environment. These research themes can also help the Department of Commerce's efforts toward implementing rigorous and detailed security control programs for the federal government. Areas where future research is needed are amplified so government regulations on information system security controls can be modified. Subsequent laws in the privacy, data protection, and medical areas are further examples of the importance of government intervention to moderate social behaviors. Despite the success of the many technical solutions that have been developed as information security controls, the human dimension has not received comparable research attention (Fraser, 2007).

The loss of control implications faced by moving toward open standards and free information sharing are areas that can learn from this research to ensure we do not repeat the security management mistakes of the past. People remain the weakest link so a comprehensive information security management or governance program is considered the best risk management option to gain optimum efficiency and effectiveness (Conner,

Noonan, & Holleyman, 2003). In chapter 3 details are discussed on how the qualitative case study is designed to uncover seminal themes and validate them through a survey instrument. A synthesis of informed opinions was developed so that information can be used as strategic guidance in developing governance rules to protect broader societal interest.

Summary and Overview

The problem society faces in trying to find balance between the need to innovate and protect society from information security vulnerabilities is introduced as the basis for the research study. A general introduction to the problem area and brief highlights of supporting literature was provided in chapter 1. This chapter covered a statement of the problem and background information on why the problem needs to be addressed. The purpose of the study explains the reason why the study was conducted. The theoretical basis used as supporting or conceptual rationale was also outlined for this qualitative study. The purpose section indicated why the study was performed and assumptions or conditions for the study are explained along with listing scope, delimitations, or limitations. The nature or design of the study is briefly highlighted and all technical terms that may not be familiar to average readers were explained. Research questions that are used to guide the study were outlined and in the significance of the study section explanations were provided to explain how the results benefit and bring about social change.

The chapter 2 literature review begins with an overview of the content, organization of the chapter, and a brief explanation of the general research strategy. The

chapter is focused around three basic research questions and the content of each section is organized to present information in terms of management and behavioral theories, federal government foundational legislation, and literary governance research. In the literature review the problem is explicated through the proposed research questions and deductive analysis conducted to reveal seminal themes, ideas, and opinions. The most representative sampling of literature was chosen to provide sufficient background information. The final section summarized the highlights of the literature that support the research study and identifies the synthesized themes.

Chapter 3 begins with an overview of the chapter and then provides a detailed description of the research design and research approach. The target population is described by explaining their major characteristics and nature. The type of sampling procedure and why it is chosen is explained and the demographics of the sample that will be selected are described. In the instrumentation section, the data gathering tool that was used is described, as well as, explanations of how validity and reliability were determined. In the methods section every aspect of how data was collected and what method was used is explained. The final section described how the data was presented and analyzed in descriptive or statistical terms.

Chapter 4 presents the results of the analysis that was conducted to address the major research questions. Results of the pilot study, descriptive statistical analysis, and correlated analysis was presented for the three basic research questions used to frame the overall research study. The chapter concluded with a summary of the barriers to

establishment, potential benefits, prevalence, and associated critical success factors. Positive affirmation, deviations, or surprising responses were also analyzed and assessed.

Chapter 5 briefly discusses the research problem, challenges, and theoretical model and framework used to conduct the research. In the research analysis section direct responses to the three research questions was provided to aid federal government managers in developing their own security policies and guidelines. Implications for social change were described, recommendations for action offered, and my reflections as a researcher expressed. In the concluding section 13 key and essential management and governance principles that resulted from the research analysis were presented. These 13 principles represent the proper fit between laws and policies, governance, and management and behavioral considerations that can be used to guide security management in the federal government.

Chapter 2: Literature Review

The research approach followed in this study describes identifies a method for finding the proper fit for principles that can be used to moderate human behavior in the midst of social change. McGregor's (1960) X and Y theories were used as a lens to discuss and implement the best set of management controls that will influence employee behavior. The controls needed to motivate the Theory X (unmotivated) employee and the Theory Y (self motivated) employee must be balanced to achieve organizational goals and objectives. This balance was referred to by modern managerial theorists like Drucker (2008) and Fayol (1987) as the proper fit. The proper fit is indicated in overlapping region of the Venn diagram (Figure 2).

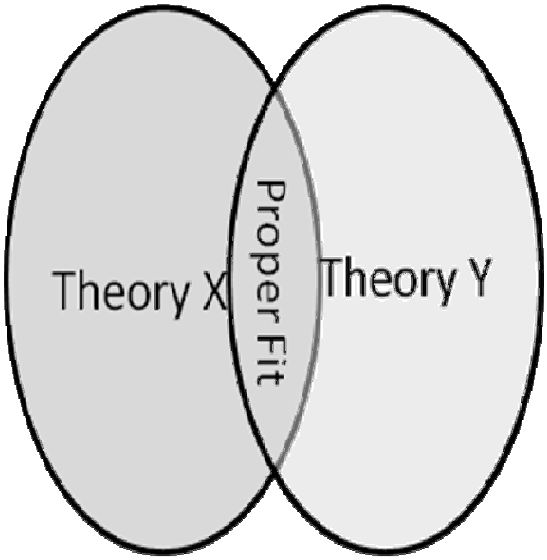

Figure 2. McGregor theories

This literature review discusses the proper fit between managerial behavior theory, FISMA, and governance principles. The proper fit would identify the set of principles or themes that can be used to make employees adhere to information system

security guidelines (Fayal, 2008). The framework supports a statement suggesting that a balance can be achieved in order to meet specific organizational goals and objectives (Fayol, 2008). The proper fit for information system security management is depicted in the overlapping region of the Venn diagram (Figure 3). The purpose of this research study was to uncover those seminal themes that can be used to strike the proper balance for moderating employee behavior.

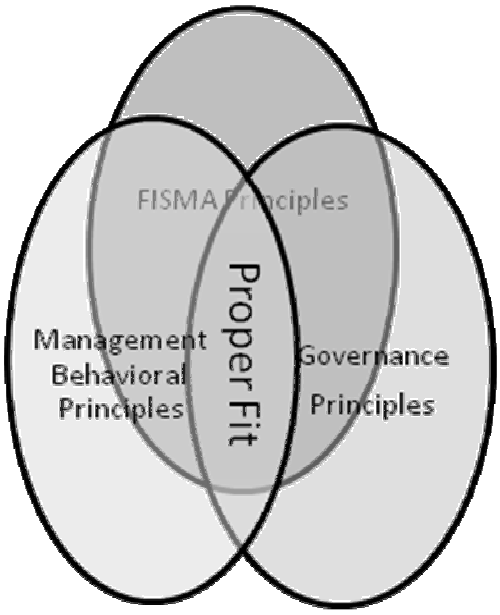

Figure 3. Information systems security principles

As indicated in the above diagrams, the literature review contains management and behavior theorist's views, federal government founding information security legislation analysis, and scholarly governance research information. The management, behavioral, and sociological theories of McGregor (1960), Fayol (1987), Weber (1962), and Hertzberg (1989) are used as the theoretical lens in which the issues surrounding

information security management are viewed. The principles established in the Federal Information Security Management Act (FISMA) of 2002 are outlined as baseline thinking on ways for organizations to improve information security management. Leading scholar's views on governance are described to complement the management and legislative views on establishing guidelines to better manage information security issues in the midst of continuous social change.

A Boolean search strategy was used with keywords such as: *management theory, behavioral theory, information security, information security management, information security governance*, and *the federal information security management act*. The search strategy identified suitable books, peer-reviewed journals, dissertations, articles, and related documents to complete the literature review chapter. The search criteria dates were set at a year range between 2004 and 2010. More than 2000 results were returned using this approach so further discriminators were applied. A search engine feature was selected that screened out results that were not peer reviewed and not full text articles. Using this feature returned several hundred results. In order to further refine the search results the specific categories of information technology, management, and decision science were selected. This level of screening provided fewer than 100 results.

Sorting search results by author, title, and date was used to consolidate similar research material. Each search displayed the databases that provided the most hits (results) so the next step was to focus on those specific databases such as Sage Journals Online, ABI/INFORM Global, ProQuest Central, Academic Search, Communication & Mass Media Complete, and Business Source Complete. This research strategy was used

repeatedly. The article abstracts retrieved from the search results were reviewed and those of interest were saved in the search engine's file management database system for later review. After saving many articles in categories such as management, information security, governance, and FISMA, each abstract was read again and articles of interest downloaded and placed on a removable storage device for printing and detailed reading. The articles that provided relevant information in response to the research questions and problem statement were selected as initial citation references.

The literature review was organized to explore information from three perspectives: human management theory views, FISMA contributions, and IT governance. These perspectives were chosen to align the research study with the research questions that were selected to guide the overall study, design, and methodology.

1. How can management practices in the federal sector be improved in response to current and emerging IT security issues?
2. How has FISMA contributed to improving IT security governance and management?
3. Why are IT security governance practices not more effective in responding to current and emerging security threats?

McGhee (2008), Nnolim (2007), Lamour (2008), and Wu (2007) dissertations were also used to guide organization of the research study. These dissertations addressed information security frameworks, governance methodologies, training effectiveness, and discussed measuring relationships between governance and effective security. Although the importance of the individual user was recognized in these dissertations, the research

did not focus on specific human or behavioral management theories that could be used to guide the development and refinement of methodologies or frameworks. This literature review was organized to focus on that gap and to uncover the seminal themes that can lead to improved information systems security management and governance.

Human Management Theories

The management, behavioral, and organizational principles developed by theorists such as Drucker (2008), McGregor (1960), Fayol (1987), and Weber (1962) can be helpful in selecting information security governance controls. Working to achieve balance between the needs of people and organizations was a challenge many decades ago and continues to plague managers in today's information age society. The knowledge worker term is used today, but McGregor's (1960) theory X and theory Y principles of long ago recognized the need to value an employee's knowledge. In order to improve information security management practices, it is important to be able to understand the individual worker's behavior in response to implemented security controls (Baker & Wallace, 2007). The following are examples of some of the challenges and concerns managers face.

Just as earlier management theorists looked at the need to integrate the efforts of people and management toward achieving common goals, information age managers have similar challenges. Information age managers needed to gain symmetry in the work force and align behaviors so information security policies were accepted as behavioral norms (Drucker, 2008). Changes in staff and line management relationships is an example of how past and present management principles are aligning in response to

information security concerns. The individual worker has become as powerful an element in the organizational structure as staff managers (McGregor, 1960). Consequently, top-down guidance and direction is not as effective as it once was in organizations. Related to information security, managers are struggling to find ways to get consensus on what the proper set of information security controls should be and decide how to build synergy (Hersey, Blanchard, & Johnson, 1996). Although organizations have accepted the need for comprehensive information security policy documents, those that are created without line input may fail because staff collaboration is essential to have a chance for success (Hersey et al., 1996). Hersey et al. went on to express that the knowledge workers of today expect lateral communications and despite attempts to control information the Internet makes limiting the flow of information difficult.

Staff and line management relationship changes dealing with responsibility, accountability, and top down communications are more examples of new challenges. The power has shifted to staff workers because their knowledge is essential to achieving organizational goals (Hersey et. al., 1996). Drucker (2008) stated that responsibility and accountability are not just central to line managers but require staff collaboration. Workers do not respond to line direction without questions and offering recommendations as the knowledge experts. Lateral communications, or collaboration, is expected (Drucker, 2008).

The Internet has also impacted management practices as more information is made accessible to people throughout the organization and external business players as well. Hersey et al. (1996) asserted that ensuring equal and timely access is a prime

concern because competitors of yesterday are business partners today. Information sharing for innovation is another factor that concerns today's information organizations.

Mintzberg (1989) explained that past managers created information domains to share information with partners and protect them from others. Security controls were needed in many different forms to deal with manager's diverse information sharing needs within and outside those domains. Mintzberg furthered research thinking by introducing a framework that listed degrees of control that extended from the extreme of nationalization to no regulation. Mintzberg stated that as early as the 1980s the objectives of the corporation and interests of society were in misalignment and required government involvement. Organizations driven by the desire to achieve goals, make profits, or innovate to gain competitive advantage struggled to balance these needs with people, organizational change, and social considerations.

Mintzberg (1989) believed innovation required information sharing both laterally and horizontally within and outside the organization. The basic organizational theory and management perspective espoused by Mintzberg and Drucker (2008) favored direct control from outsiders like shareholders to mediate the profit oriented nature of business. Drucker (2008) asserted that despite the need to innovate, management is truly about people, their knowledge, and relationships. Governance, as a form of control, was mentioned by Fayol (1987) as one of his key sub specialties because of its importance in moderating behavior and working activities. Fayol also supported Drucker's assertions by stating that there is no known formula for success; however, the information sharing theories of the past should be used to inform future management decisions.

In addition to the human management concerns brought on by the information age, human behavior studies are also relevant to keep employee and management goals in balance. Sociological thinking espoused by Weber (1962) dealt with the interpretative understanding of human behavior. Interpretations or observations were used to try and explain behavioral responses; however, there was no conclusive evidence that the stimulus drove a particular response. The new social norms, ethical values, and cultural trends from Chung's (2007) research revealed behaviors that are having impacts throughout society. Based on Weber's thoughts, observation, and analysis of these types of behaviors, they are important considerations but conclusive reasons beyond just an intellectual understanding should not be sought. Weber's point is that although largely subjective, interpretative analysis is another tool that can inform managers in making policy decisions.

Weber (1962) explained that various sociological interpretations and observations are used to explain why certain behavioral responses occur. Weber referred to the match between a behavior and response as an ideal type, but accepted that there are no known methods for knowing outcomes based on inputs when it comes to managerial theory. Understanding is an important sociological principle, although subjective, it is a tool that can help in sociological research for interpretation and observation (Weber, 1962). Weber also believed that social conduct must have an orientation to the conduct of others to be meaningful.

Cooner, Noonan, and Holleyman (2003) introduced the notion that past organizational management was more a command and control type activity; however, it

has taken on more of a legally defined construct. Societal governing influences are causing organizations to change their management approaches to comply with laws that are aimed at protecting the common good of society. Managers face challenges in the new environment that are comprised of social markets, customers, and technology. It is increasingly difficult to gain a competitive advantage and distinguish yourself in the market place (Conner et al., 2003). Information security management challenges seem to further complicate matters as more controls are required. FISMA and the National Institute of Technology (NIST) publications that direct federal security controls are a form of legal guidance. The Sarbanes-Oxley legislation and Health Insurance Portability and Accountability Act (HIPPA) of 1996 rules are two more examples of how a legal construct is guiding management and organizational actions.

Conner et al. (2003) explained that there is a definite distinction between autonomous and entrepreneurship organizations. Each organization is affected differently by these legal or policy changes. The autonomous organizations need performance measurements to maintain control and entrepreneurships must focus on capital formulation controls. The impacts to these two different organizations would be different, based on the type of legislative controls levied, but could have grave consequences on their ability to sustain themselves. For example, information security legislation can be costly and troublesome in finding and hiring specialized experience to launch a new business venture and meet regulatory guidelines (Conner et al., 2003). Conner et al. also suggest that society may not be able to trust businesses to forsake profit in the interest of the common good. Mintzberg's (1989) response was that stockholders are essential

leaders that can moderate business leader's behavior and preclude governmental regulation that attempts to level the playing field.

Management of the past and future is still about control, authority, and motivation of people to achieve organizational objectives or goals. Striving to achieve balance between the needs of the people and organization remain a central challenge (Mintzberg, 1989). Instead of focusing specifically on controls, theorists suggest a slight shift to performance measures (Drucker, 2008). Drucker believed the knowledge worker is more a Theory Y person and is eager to work toward accomplishing organizational goals. It is therefore important to seek a balance between the needs of the organization and the knowledge worker for the organization to perform effectively. Drucker stated that performance objectives, when applied properly, can integrate the efforts of people and management to work together to achieve measureable goals that contribute to the core mission of the organization.

Fayol (1987) asserted that there are no known formulas for success in management; however, developed theories and principles should be used to inform and guide decisions. Past theories should help in devising new approaches and solutions to management challenges. As managers develop strategic plans, Fayol offered five sub specialties that warrant their attention. Economics, production, governance, human relations, and cybernetics are the areas that he believed encompass the major management considerations for most businesses. Fayol also stated that managers should create basic lines of authority, issue commands, establish priorities or sequencing, and then monitor and correct actions as appropriate. He further stated that all activities in

business management can be included in a framework of technical, commercial, financial, security, accounting and managerial functions. Strategic planning that includes information security can be greatly simplified by starting with such a functional framework. Using this type of framework, the strategic plans will provide unity, help avoid confusion, offer flexibility, continuity, and improve accuracy (Fayol, 1987).

Hersey et al. recognized that knowledge is the key resource that must be managed to affect organizational change. The organizational landscape is changing to require more upward mobility opportunities, continual training, changing demographics, and various political, economic, education, and other challenges. These landscape changes reemphasize the earlier point made that there is no one way to manage and the scope of organizational management is moving from a purely command and control to a legally defined construct (Conner et al., 2003). Societal governing influences are placing stipulations on organizational management to protect the common good and enforce compliance with laws. Another landscape change is seen in business profit allocations. Situations range from monopolies to autonomous organizations like the military. Management theorists seem to supports the notion that public regulation control is essential for monopoly situations and conversely, autonomous organizations will spin out of control if they do not have performance measurements to drive them (Hersey et al., 1996).

Social impacts in businesses are caused by new innovations or technological improvements (Drucker, 2008). These impacts are proving to be a double edged sword as they are essential to stay competitive, but can force controls that are very costly and

troublesome. A new business venture can be expensive, require new knowledge, and specialized expertise. Mintzberg (1989) described the need for a new pluralism to balance special purpose and common good needs. As an example, entrepreneurship situations are focused on capital formulation and control because it is essential to their ability to maintain operations. Entrepreneurships must still innovate to stay competitive so these goals become self regulating performance objectives that steer their decisions. Mintzberg explained that the issue is also one of trust that the business will not forsake common good principles for the benefit of profits. Since business leaders are essentially controlled by their stockholders it is hard to believe profits will be reduced to meet social good causes without some form of controls being applied by external agencies. The next section delves deeper into specific management principles and theories on human behavior, organizational management, and social behavior.

Predicting and Controlling Human Behavior

Managers are hampered as they try to innovate using humans because adequate conventional theories on organizational behavior do not exist. McGregor (1960) believed that continuing to analyze and discuss management theories will allow room for continued improvements though collaboration to develop new ideas and innovations. McGregor described management as "the ability to predict and control human behavior" (p. 4). The central principle of theory Y is integration to create conditions so the organization can achieve its objectives. Integration means both the needs of the organization and individual must be addressed. The key assumptions from theory Y are:

> expenditure of physical and mental effort in work is as natural as play and rest, man will exercise self-direction and self-control in the service of objectives to which he is committed, commitment is a function of the rewards associated with their achievements, people learn, under proper conditions, to accept and seek responsibility, capacity to be imaginative, creative, ingenious in solving organizational problems is widely distributed in the population, in modern industrial life, the average intellectual potential of average humans is only partially used. (McGregor, 1960, p. 47)

A broader theory Y approach is applied to the whole organization instead of just individuals and groups. The key is to develop performance objectives in which measurements require combined efforts to achieve success. An example of such an objective would be to quantitatively improve the economic success of the organization. The measurement would factor in the necessity for individual and group contributions so it would be clear that a collaborative effort was essential to success.

Another important management principle is control. Managers seek certain control methods in order to adjust or manage the behavior or actions of their people. McGregor (1960) believed control must be selective, or appropriate to the nature of the situation or circumstances. Using or selecting controls require precision because human behavior is influenced by so many different factors. Incentives are where managers often choose a control measure that is in direct violation of human behavior. Financial incentives alone are seldom effective for long-term behavioral changes or sustained

performance improvements (Drucker, 2008). In addition to the normal human behaviors that require management attention, external considerations like professional ethical values must be factored in. The manager's ability to make decisions has progressively been reduced. Legislation like the child labor law, women's employment rights, and collective bargaining are examples of some of these external considerations.

Fayol (1987) used the term cybernetics to address the ever increasing availability of information used in decision making processes. This information represents the "keys to the survival of an organization and its ability to adapt" (Fayol, 1987, p. 4). Future challenges in cybernetics are to establish information systems, generate appropriate data, separate applicable information from massive flows of data, identify the needed decisions, and make decisions according to established rules, processes or methodologies. Fayol (1987) stated that companies that can adapt, measure its output, provide feedback to the input, and change the output as needed will avoid organizational fractionalization, obsolescence, or economic destruction. These cybernetic concepts of control are the monitoring and coordinating elements of Fayol's progressive management theory.

Staff and line relationships and the principles of authority are key considerations that affect a manager's ability to control human behavior to achieve company objectives. McGregor (1960) asserted that authority must be equal to responsibility (p. 146). On the other hand, too much authority can be counter productive and you should delegate. Nonetheless, managers can never delegate the responsibility for completing a task or accountability is lost. McGregor believed that authority is widely used as the central form of persuasion or control. McGregor stated that many of the textbook management

principles actually conflict with management theory. Principles like hierarchical structure, authority, unity, and task specialization are not effective in controlling behavior. These conventional principles come from old models developed in the military and churches. Today's knowledge worker's behavior and motivations are more complex. Regardless of the authoritative method used, "success depends on altering the ability of others to achieve their goals or satisfy their needs" (McGregor, 1960, p. 20).

In terms of motivating people to perform, McGregor's (1960) theory X principles still seem to be solid foundational tenants. In fact, these principles represent a traditional view of direction and control. Three descriptions can be used to summarize the theory X principles. Theory X posits:

> average human beings dislike work and will avoid it if they can most people must be coerced, controlled, directed, threatened with punishment to get them to put forward adequate effort to achieve organizational goals or objectives, average humans prefer direction, wishes to avoid responsibility, and have relatively little ambition and want security above all else. (McGregor, 1960, p. 33)

People are considered naturally wanting animals so they crave attention to give them the impetus to act. Human need is a hierarchical function that has dependencies and interacts with the elements above and below in the hierarchical social structure. An important assumption is that those needs which have already been satisfied are no longer motivators of behavior. The next section takes a closer look at management with a focus on human resources.

Human Resources: People, Process and Technology

Drucker (2008) believed management of the organization's resources is the primary means in which the firms are able to achieve their objectives. The resources include its people, processes, and technology. Each of these resources require different tactics; however, they must be addressed individually and then in an integrated fashion to gain the most benefit for the organization. As a liberal art, Drucker explained that management is concerned with people and power, values, structure, constitution, and most importantly responsibility. The people, as the most important resource of the organization, must be empowered to carry out the tasks of the organization with supervisory guidance and assistance.

Aside from their personal values that will affect task completion the values of the organization must be well understood so the people can work independently to accomplish daily tasks. The organization, no matter its mission or focus requires some form or structure be established to guide actions and address concerns. Drucker (2008) stated that constitution is the affirmation of organizational principles that define the purpose, goals, and intended behavior of the unit. It is also accepted that strategic plans often provide the overriding guidance that helps constitute intended behavior towards a common vision.

Drucker (2008) asserted that the definition of management is to make human resources productive (p. xxxiv). As we manage in the information age, workers are no longer seen as production workers, but knowledge workers. The largest group of workers in the United States is believed to be knowledge workers. The workers no longer have a

production mentality but associate themselves with a company by their profession or specialty. For instance, people refer to themselves as database administrators, carpenters, salesmen instead of saying the name of the company that is their employer. Collectively, managers and the people who make up the organization's principle mission are there to serve society (Drucker, 2008). By serving society, managers are able to turn social dysfunction into business opportunities. In terms of social impacts that are negative influences, leaders and managers must work to obtain appropriate regulation to level the competitive playing field. Drucker reminded all managers that it is their core responsibility to seek regulation instead of having it thrust upon them.

Edersheim (2007) expressed that Drucker's (2008) management philosophy revolved around five main themes. He believed you had to connect with customers, prepare for technological innovation and abandonment, develop lasting collaboration, attract and grow knowledge workers, and establish a disciplined decision making process. These principles reflected his modern thoughts on management of knowledge workers in the information age and looking toward the future. Chief executive officers, as the managers and leaders of the company, have the inherent responsibility to institute these principles. The chief executives should focus on bringing the outside in to ensure the company understands the views of the market place (Edersheim, 2007, p. xi).

According to Drucker (2008), successful innovation entailed developing responses to four important questions: (a) What do you have to abandon to create room for innovation?, (b) Do you systematically seek opportunities?, (c) Do you use disciplined processes for converting ideas into practical solutions?, (d) Does your

innovation strategy work well with your business strategy? Companies often make the mistake of trying to innovate without changing existing business operations and end up with negative growth. The company has to give up some of its current operations in order to add innovative solutions. The trade offs are hard decisions, but can be simplified by openly accepting the need to change strategic objectives. A company that is systematically looking for opportunities in its workspace has the best chance for finding individual or collaborative ventures that offer growth potential (Edersheim, 2007). The following section reviews important points about how change in society affects the employee and organization.

Change Management Dynamics – Knowledge Worker

Theory X principles offer a strategic framework upon which managers can build effective motivation strategies to deal with changes in employee behavior and organizational structures (Drucker, 2008). McGregor (1960) explained that the philosophy of management that relies on direction and control techniques is inadequate to motivate people. The human needs which underlay these techniques are no longer important to today's knowledge worker as they were in the industrial age. McGregor also explained that theory X is not meant to be a description of human behavior but it is consequence based. The principles and assumptions are not statements intended to characterize individuals but give a theoretical representation of reactions to certain motivators.

McGregor (1960) recognized that the two theories have aged; however, feels they should not be excluded in today's management environment. The theories should be

studied so new techniques or innovations can be discovered based on these founding research principles. For example, theory Y in practice is synchronous with the management by objectives concept. In both concepts you clarify broad requirements, establish specific targets, establish management processes during the target period, and evaluate the results. In other words, you tell people what to do, judge them, and then reward or punish to control behavior (McGregor, 1960). A contrasting theory X approach would be to determine what is needed to motivate and then provide or withhold the motivator to exercise authority or control.

As far as making profits is concerned, Drucker (2008) taught that the money follows knowledge so managers should focus on providing leadership and direction (p. 13). This focus would in turn allow them to be profitable in their pursuits. Drucker also believed managers should ask themselves what is your business, who's the customer, and what does the customer value. Answers to these three questions would keep the company grounded and developing strategies which fit the present and future needs of the company and its knowledge workers; despite change. Objectives are still seen as the guiding lights in a strategic plan (Drucker, 2008). Management by objectives is still a very effective technique as long as the objectives have been well thought out and articulated. In order to have a knowledge environment, managers must teach their people how to learn. In other words, mature methodologies, processes, and procedures must be in place to guide the learning process. These actions ensure knowledge is productive and actionable instead of there being a lot of information. As an individual knowledge worker, Drucker (2008) suggested you know your own strengths and collaborate to

enhance your weaknesses. Every now and then, ask yourself what do you want to be remembered for and the answer can keep you synchronized with the company's goals and objectives.

Recognizing the impact the Internet boom has in causing changes in business management, Drucker (2008) espoused the importance of noting the changes across the horizon that come as consequences of the Internet. Access to the tons of information is not the most important point for managers to concern themselves with. Societies must change many of their fundamental ways of acting, thinking, and characterizing actions as information becomes accessible in ways never imagined (Edersheim, 2007). Edersheim explained that there is a new solution space that describes competitors as business partners engaged in finding unique ways of putting solutions together. These solutions are what society sees as value and hence they provide business opportunities for companies to pursue.

A company is nothing more than its people, their knowledge, and relationships (Edersheim, 2007). This line of thinking reinforces previous thoughts on the need to move away from the production worker mindset and recognize a new change dynamic is in play. The motivators for behavior, acceptance of responsibility, desire to succeed, and general attitudes toward task completion must be handled in a different manner. Edersheim concludes that more inclusiveness, interdependence, and collaboration between managers and the people inside and outside the company are in order.

Organizational Behavior: Changing Society

Today's managers are facing new challenges as a new information work force has emerged. Knowledge is now the key resource to be managed as businesses face borderless environments on a global scale. The business conditions must support an upward mobility opportunity for most workers and the potential for failure and success is probably more evenly distributed than ever before. Capitalization is more prevalent as startup companies own their own production means and seek access to organizations for specialized services or knowledge. Knowledge is also rapidly becoming obsolete as new innovations, procedures and processes are introduced so today's knowledge worker must constantly reenter the training cycle to stay current and offer a competitive knowledge advantage (Edersheim, 2007).

Hersey et al. (1996) indicated that changing demographics are another dynamic that requires management attention. Age, low birth rates, and overall lower population size along with immigration challenges are factors that must be considered. These factors threaten to change the base landscape of our society. Economic impacts, new political bases, health care, finance and education are areas that have to change in response to these changing social conditions. Organizational factors referred to as contingencies also drive external and internal change. Brown and Grant (2005) explained that organizational size, industry, and specific business strategies should moderate governing policies and procedures to find the optimum management model. The next company is not a single firm but will be comprised of several different companies that have related interests.

Outsourcing of information technology services to lower physical communications costs is one real example of a major response to changes in the business world that resulted from changes in social conditions (Hersey et al., 1996).

The new reality asserted by Hersey et al. (1996) is that in future corporations, people, policies, and outside information will all become change agents. These agents are forcing a disintegration business strategy as opposed to the integration approach used now. Outsourcing is an example of disintegration and Goo (2009) stressed the importance of relational governance as a way to enforce obligations, promises, and meet trust and social identification expectations. Strong relational governance is believed to replace the need for formal contracts like service level agreements because sufficient trust exists between the two business partners. The belief that there is one right organization and the meaning of management refers to business management, are false concepts as future challenges unfold (Goo, 2009). Similarly, management theorist like McGregor (1960), have long stressed the principle that there is not one right way to manage. It would appear that managers must shift their thinking to managing performance as opposed to people.

Hersey et al. (1996) pointed out that technology is also not specific to one particular business firm or industry. All businesses, in their new disintegrated form, must find ways to advance themselves through the use of technological innovation. A major theoretical assumption going forward is that all technology will be important to every industry. The scope of management is also not just a matter of command and control, but has shifted to become more legally defined. In fact, businesses could be considered more

legal entities than organizations controlled expressly as management structures (Hersey, et al., 1996).

Reading the warning signs of changes in management theory dictate new thinking to deal with rapid growth and still achieve business objectives (Drucker, 2008). The theory of business teaches you to stay focused on the environment. Our future environment is characterized by society, markets, customers, and technology. Hersey et al. (1996) believed there are four specifications that relate to core management competencies. The business assumptions must fit reality, the theory must be known and understood, theory must be constantly tested, and the assumptions, theory and testing mechanisms must fit one another. All in all, change must be embraced as an environmental factor which offers competitive advantage and distinctive business opportunities.

Service institutions are by far the most prevalent organizations in our global society. Fifty percent of the gross domestic product, from the United States and developed countries, goes to service organizations (Hersey et al., 1996). Mismanagement has occurred when businesses were run for the convenience of the employee instead of looking at specific employee contributions to performance. Organizational or business profit allocation issues are also important factors that must be understood and controlled. The controls may be implemented by corporate leaders or through regulation. For example, a natural monopoly's budget is best controlled under public regulation. Public ownership is also feasible; however, this method is usually reserved for more extreme monopoly situations. The assumption driving this thinking by Hersey et al. was that an

unregulated monopoly will eventually exploit the market place. If ownership control is placed in the government the exploitation concerns are addressed; however, there is little redress for inefficiency. Therefore, logic suggests that an independently managed monopoly under public regulation should be more responsive to customer needs.

The military is an example of an organization that operates with a large degree of managerial autonomy. Although there is management autonomy these type organizations must have discipline of objectives, priorities, and produce measureable results. It is difficult for these type organizations to commit themselves to real abandonment of obsolete methods to make room for future innovations. These organizations seem to grow larger, as innovations are integrated, because of the social difficulty in deciding what objectives must be set aside. In comparison, if nonprofit organizations are to perform successfully they must develop continuous improvement habits, be open to changing its basic structure as the size of the organization changes, rethink itself if it is over 40 years old, and review outgrown policies and rules of behavior (Hersey, et al., 1996). Organizations that do not change its habits become ungovernable, unmanageable and uncontrollable.

Hersey et al. (1996) explained that entrepreneurship is another important management challenge in public service institutions. These organizations need vibrant engines of capital formation so they can sustain their basic organizational structure. Capital control or management is the most important initial concern so they must be frugal and work hard to prevent waste. Innovation is still necessary to efficiently achieve objectives but the controls placed on capital require more precision in deciding what, how

and when to pursue opportunities. In a sense the entrepreneurships are more self regulating and focused on performance objectives because their capital is often more limited. Hersey et al. believed that the monopolies and government organizations can learn from this type of capital control, management, and governing structure.

In all businesses there are obvious social impacts and responsibilities that must be embraced by managers and leaders. Social impacts are those impacts to the institutions themselves and problems introduced into society itself. The amount of responsibility has been an important point of debate and remains so even today. The first cars were not manufactured with seat belts; however, after concerns for safety were expressed in society, seatbelts were included in all cars under government mandate. Since people did use the seatbelts, further government regulation made use of seatbelts mandatory for all drivers. This example demonstrates that social impacts come from innovation and for the better good of society require restrictions be implemented to take advantage of the innovation. In other scenarios the restrictions can be more costly to manufacturers and hence drive up the cost of the innovation that could potentially make it less desirable to the consumer. Hersey et al. asserted that it is a prime responsibility of management to get appropriate regulations passed to address social problems.

In developing new business ventures managers must factor in the social impacts early on. The expense, specialized knowledge or expertise requirements should be part of the development decision matrix. As impacts are identified, solutions or mitigation measures must be included in the business plan. The difficulty is determining what illegitimate costs managers should resist in solving social impact problems. Hersey et al.

(1996) stressed that the overall responsibility lies with the government because the benefit and impacts to society must be rationalized.

Research by Hersey et al. (1996) showed that multipurpose organizations do not perform efficiently so there is a real need for more pluralism. Conversely, as more pluralism is embraced it is crucial managers look beyond their traditional borders and accept a true sense of responsibility to serve the common good of society (Hersey, et al., 1996). Ionescu (2007) added that effective management is at the heart of organizational performance and success. A critical change management challenge is aligning market forces with organizational values. This alignment is important because it supports building shared values, beliefs, and perceptions of the security environment. Change discussions continue in the following section as information sharing within and external to an organization is discussed.

Organizational Information Sharing and Control

Mintzberg (1989) explained that there are several challenges managers face as they strive for more effective management. Managers want to find more systematic ways to share their privileged information. Because they need to leverage business opportunities through relationships it is necessary to create shared information domains while maintaining their own privacy and protecting information shared in other relationships. It is also important to have mature processes in place so serious attention can be given to important issues. It is not just the details surrounding an issue but managers need an ability to step back and take a broad view of the entire situation. The

effective manager will be able to detect discontinuity, manage patterns, and reconcile change and continuity (Mintzberg, 1989).

Mintzberg (1989) explained that formal information is often inadequate to fully satisfy the information needs of a manager. The information is too limited, general, late and unreliable. Due to meeting time constraints information is usually paired down and presented in general terms instead of detail. During this process, assumptions are made that reduce the reliability and validity of the information. Outside perspectives are usually missing as well. Often it is rigid and dysfunctional objectives that encourage the continued use of information even though it is not helpful in advancing the most important business objectives. Also, politics often distorts information that is presented in certain reports. A report prepared for presentation to a customer will probably not emphasize the negative aspects of a situation. Politics in organizations are, by their true nature, divisive influences and these influences pit individuals or groups against the system.

In our society of organizations, Mintzberg (1989) explained that life cycle models suggest that as organizations grow and become larger they tend to seal themselves off from external influence. In essence, they become powerful closed systems under the control of their own insiders. Control of corporations comes in many different forms for various reasons. Corporations could be nationalized under government control or simply under shareholder control to focus on private economic goals. They could also be democratized to open up business operations to larger and widely held corporations. Regulating the corporation could also be introduced to emphasize a social goal focus.

Based upon past legal issues, leaving the corporation to self regulating influences and natural controls does not appear to be the most effective method (Conner, Noonan & Holleyman, 2003).

Basic organizational theory supports the notion of having direct control from outsiders like shareholders to help better mediate or control the profit oriented nature of business. Mintzberg (1989) prepared a horse shoe framework to help managers see the dynamics and extremes of non regulation to full regulation or control. The framework lists degrees of control from nationalize, democratize, regulate and pressure on one side of the horse shoe. On the other size of the shoe are restore, induce and ignore tactics. In the middle of the shoe is a center of trust or no regulation or control. The framework explains progressive control actions that can be taken to regain control of a situation, provide moderate oversight, and give complete trust; no control.

Choosing to naturalize would be a viable option if mission or services are not adequately provided by a private company. This approach does not necessarily improve economic or bureaucratic problems but attempts to restore creditability in services. Telephone, utilities, railroad and Amtrack are examples of nationalistic service implementations throughout the United States. Mintzberg stressed that the requirements should be the determining factor and they must be linked to government policies that are managed by the state entity.

When corporations face economic pressure the social good cause seem to lose out without outside intervention. Mintzberg (1998) asserted that "a society with only a legal scale is one not worthy of man" (p. 318). In other words, corporations must be trusted,

within reason, not to take undue advantage of societies. The decision to do nothing is not viable because it is non responsive. Regulation, on the other hand, is a response to return direct control of ownership to the stakeholders. This tactic keeps free enterprise and freedom principles safe and avoids the unpopular circumstances of socialism. In essence, it seems the fundamental concept is the need to make trade off decisions to balance economic and social goals.

Comprehensive Framework: Federal Information Security Management Act (FISMA) of 2002

This section describes the Federal Information Security Management Act and discusses how it was designed to improve IT security governance and management. The federal information security management act (FISMA) of 2002 was enacted into law to provide a comprehensive framework to ensure the effectiveness of information security in the federal government. The act recognized the complex nature of security and the importance of including coordination requirements with civilian, national security, and law enforcement agencies. The act was structured to provide minimum controls, improved oversight, use of commercial products, and delegation of specific responsibilities to individual agency leaders. In the broadest sense, the act was focused on ensuring integrity, confidentiality, and availability of information security services. The director of Office of Management and Budget's (OMB) authorities were increased to include ensuring timely agency adoption of and compliance with standards that would be promulgated through the department of commerce chairman by the national institute of standards and technology director.

The director was also charged with overseeing agency compliance, approving security programs, coordinating policies, managing a federal information security incident center, and reporting to congress on actions taken to address deficiencies. The federal information security incident center was chartered to provide timely technical assistance, compile and analyze information, inform agencies about security threats, and consult with National Institute of Standards (NIST) and agencies that are operating national security systems on behalf of the President. Authority for a special category of systems specified as national security systems was delegated to the defense department and central intelligence agency.

FISMA (2002) outlined the general and specific responsibilities of all federal agencies. In general the agency heads must provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems. The focus of the management programs was to reduce risk to an acceptable level and periodically test and evaluate programs. The chief information officer had previously been delegated information security management and oversight responsibilities under the Clinger-Cohen act. Therefore, at the agency level the Chief Information Officer (CIO) was expected to appoint a security director or carry out these new duties themselves. FISMA required the various agencies to have independent audits of their security programs performed at least annually. NIST was clearly given the responsibility to prescribe standards and guidelines on federal information systems. NIST was directed to develop mandatory standard to ensure the minimum information security requirements

were enforced. Authority to disapprove or modify these mandatory standards rests solely with the president.

FISMA's purpose and directions to the federal government agency leaders was clear and concise. The act did not override other information management authorities but complemented them (Newell, 2007). FISMA modified the information management and control authorities already given to the Director of the office of management and budget to include security. The responsibility for developing standards remained with the commerce department and their role was modified to include specific information security control standards. Mitrakas (2006) provided a European Union perspective that indicates a framework similar to FISMA is necessary to allow members of society to exercise and enjoy basic rights. Mitrakas also expressed the need for cross border cooperative agreement needed to prevent exploitation of others' framework agreements and legal rules. The NIST, a subordinate agency to the commerce department, was the technical arm charged with coordinating the development and implementation of mandatory security standards.

FISMA Regulatory Compliance: Inequities

Although the act was viewed positively, there were several inequities expressed about FISMA that deserve management attention. Newell (2007) stated that the FISMA of 2002 has standardized the methodology used to provide a consistently repeatable information assurance program for use throughout the federal government. The requirement for reporting the state of information security and a normalized scoring system quantifies the progress of maturing information security programs. The reports

contain boundary declarations, risk assessments, security plans, and security incident impact statements. In addition to these requirements there is certification, compliance level, and accreditation reports to affirm any report findings.

Despite these detailed and well structured processes and requirements Newell (2007) believed inequities still exist. Primarily the burden placed on small businesses and their customers is much larger in comparison to other companies. FISMA was basically a one size fits all act that does not give consideration to the expense small businesses must undergo to try and keep up with its constantly changing criteria. The FISMA reporting system should be further standardized and finalized so everyone can operate on the same normalized criteria. There are too many variations in enforcement and implementations between agencies to be supported by the small business community. From a small business customer perspective, the annual reporting requirements, extensive tracking, and archiving of artifact data cause a resource drain. The automation tools that have been developed help; however, they don't replace the need to hire subject matter experts that have the necessary experience and credentials. Small businesses would not normally have these type individuals under permanent employment.

Newell (2007) believed that the rigor of preparing the required paperwork to get a passing score consumes all the security planning time and often leads to nothing more than a paperwork exercise. Nonetheless, the public embarrassment of not achieving a passing score is too penalizing to take any chances. Federal organizations risk undergoing an audit and possibly forced budget cuts if they don't pass. The second phase of regulation that may require organizations become formally certified to offer FISMA

services will further exasperate the problem. If this requirement is levied it will limit the pool of potential security professionals who would otherwise be qualified to conduct this important work. Kolb (2009) added that non profit organizations also struggle to meet stringent security requirements because they can not raise money to offset these costs. Nevertheless, they have the same legislative constraints as other companies. On a more positive note, standardizing the contract language in requests for proposals will help build consistency and repeatability into the service process. Newell (2007) suggested a continued iterative approach be implemented so the consumer culture and professional service providers have time to adapt.

FISMA 2002 served as a foundational information security governance document to analyze the effectiveness of information security programs in the federal government and broader society. The structural guidance, assignment of responsibility approach, oversight agency appointments, broad coordination system, and audit control processes are excellent framework lessons for other organizational programs. Hoover (2009a) cautioned that some guidance has led to over classification of the government's cyber security actions and hampered information sharing and collaboration. This action also goes against research that suggest knowledge workers should be engaged in decision making processes and it fosters a theory X leadership style that keeps employees dependent on managers to make decisions. Hoover (2009b) also pointed out that FISMA does not require preventive security measures, demand continuous monitoring, or assess the effectiveness of existing measures. Despite a few shortcomings, if the federal government has effective security programs, it is prudent to consider further governance

legislation that may address security problems that plague others. A contrary view to the United States' governance legislation is posed by Sys (2007) as the Belarusian perspective is to treat the Internet as a serious threat to its ideology. Criminal penalties are assessed for unsanctioned access and state owned telecommunication companies are forced to control access to the Internet.

Effective IT security implementation is just a matter of "enlightened organizational self-interest" where a company seeks to protect its own information and that entrusted to it by customers, suppliers, or other partners (Conner, Noonan, & Holleyman, 2003, p. 2.). Two key items are often overlooked: responsibility is too often delegated, and the need for a framework of action to set priorities, assign task, get started, and monitor implementation. Based on Pricewaterhouse Coopers' research (2000), IT governance was implemented largely for two reasons: risk management and value delivery (p. 7). IT's contributions to efficiency and effectiveness were deemed more important than its innovation value. Organization culture was the most prevalent barrier preventing full return from IT investments. Additionally, strong IT governance practices correlate positively with better IT outcome and the majority believe IT's performance was in line with expectations.

As noted by Baird (2002), companies urgently needed to improve information quality to insure transparency, accuracy, timeliness, and reliability. Some of the specific IT research areas include: process simplification and standardization, data simplification and standardization, and technology standardization and integration. In the business intelligence, or knowledge management area, e-records management, electronic data

interchange, and supply chain activities required more process control, oversight, data storage, and accountability. The systems integration challenge may be the most difficult for IT professionals as many of the systems have been developed and modified over years and don't follow today's standardized data management methods and processes. Volonino, Gessner, & Kermis (2004) stressed that security must be strengthened to distinguish authorized suppliers, employees, and management levels so proper access privileges can be issued. Also, the security features must be monitored and alerts established to notify proper authorities when unauthorized actions occur.

Few argue that a secure and trusted environment for stored and shared information will enhance consumer benefits, business performance, productivity, and national security (Conner, Noonan, & Holleyman, 2003, p. 1). The four major findings from their research are: (a) government has already established significant legislative and regulatory regime around IT security, and is considering additional actions, (b) information security is often treated solely as a technology issue, when it should also be treated as a governance issue, (c) there is already broad consensus on the actions necessary to remedy the problem, and (d) lack of progress is due in part to the absence of a governance framework. Herath, Herath, and Bremser (2010) proposed a balanced scorecard framework that is complimentary to FISMA. The framework looks at management, users, internal processes, and future readiness in terms of goals and measures for each area. Herath et al. suggested this model is effective because it incorporates measurements that are linked to information security goals in each specific area.

Wittmann (2009) asserted the need for a more centralized approach to overcome funding shortfalls that have been the detriment of government initiatives to institute unified identity management, expanding the internet protocol numbering scheme standard, and implementing the guidance proposed under FISMA. Additionally, current and probable cultural changes in information technology are expected to occur in four areas: a) application and combination of IT to humans may lead to major cultural impacts, b) IT may lead to weakening collectivism and feeding individualism, c) individual creativity may encourage creative thinking in education to change all forms of education, and d) an iconic society may develop that relies on visual images as a key communications method (Chung, 2007).

Mandatory Security Controls

In the area of security controls, a Department of Commerce (2006a), Federal Information Processing Standards Publication (FIPS) 200 defined the minimum security controls that must be implemented. FIPS publication 200 was prepared by direction from Federal Information Systems Management Act (FISMA) of 2002 to provide standards for categorizing information systems, guidelines recommending types of information systems, and minimum information security requirements. These standards provided mandatory information security control. FIPS publication 200 listed seventeen security related areas that were defined to protect confidentiality, integrity, and availability of federal information systems.

The security-related areas include: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security

assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. (US Department of Commerce, 2006a)

The 17 areas represent a broad based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems. Before applying the security controls, the government information systems must be categorized as low, medium or high impact. This categorization determines which specific control features must be applied. The security controls must meet one of three tailored security control baselines that are associated with designated impact levels. The agency chief information officer or senior information security officer coordinates on the implementation to ensure a cost effective, risk based approach to achieving adequate security across the organization. The results of these selections must be documented in an organizational security plan.

Guidelines: Security Control Selection

The purpose of Department of Commerce (2006b), NIST Special Publication 800-53 was to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. It is very important that the responsible officials understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals.

Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of systems and its information. Managers must focus on understanding what security controls are needed, assess what controls have been implemented, and decide their desired level of assurance goals. Publication 800-53 provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies.

The publication facilitates a more consistent, comparable and repeatable approach for selecting and specifying security controls, provided recommendations for minimum security controls that are categorized, provided a stable and flexible catalog of security controls, and created a foundation for developing assessments and procedures to determine security control effectiveness. Publication 800-53 described the fundamental concepts associated with security control selection and the process of selecting and specifying security controls for an information system. The publication also follows a very detailed risk management framework to guide selection and specification of security controls. The essence of the publication lies in an extensive table that has been developed. The table lists minimum security controls, or security control baselines, for low-impact, moderate impact, and high impact information systems. This table matrix summarizes at a high level the detailed work that must be completed to meet minimum requirements for information systems categories. Publication 800-53 is a technical management document that has been synthesized into checklist form to guide information security planning, preparations, and implementation.

Internet Growth: Crisis of Governance

This section discusses IT security governance and why many of the practices are not more effective in responding to the current and emerging security challenges. First looking at the Internet, Baird (2002) described its growth as a crisis of governance that needed to be addressed. The days of thinking self-regulation will create order and self regulate are far gone. Certainly, this type of change will require the government to change its operations so it does not end up stifling innovation. Baird believed that the government's participation in managing the Internet is essential and suggests that three main changes are necessary to strengthen its governance model: government power sharing with experts in the IT community, business sector, and non profit organizations.

Conner et al. (2003) stated that a major shortfall in information security governance is the lack of a framework that explains who should do what. The authors recommend the development of a framework for action to outline manager's general responsibilities. Ultimately they feel that information security is not just a technical issue but a corporate governance challenge or responsibility. Their research indicates that there is already broad consensus on what needs to be done to address the many issues but a framework has not been developed that outlined the roles for business units, senior managers, Chief Information Officers (CIO), and Chief Executive Officers (CEO). De Haes and Grembergen (n.d.) believed these roles must be established to obtain a certain maturity level and that will strengthen the organization's ability to implement security controls through the guiding framework.

Transparent processes that earn public trust are what Baird (2002) saw as a pluralistic model for success in developing internet governance rules. The rules will then represent the interest of the three key functions: government, business, and non profits. Contrasting views have asked for the government to stay out of the business of Internet regulation because it would never be able to move fast enough to keep pace with the technological changes. Baird explained that internet innovators assert that the government does not understand the culture, ethics, and unwritten code of the Internet society. It is perhaps the tensions that have come from content regulation discussions, hate speech, and pornography that have led to disagreements about government regulation. Legal battles have also ensued as the business world competes for prime virtual real estate to advertise and sale their goods.

The new economic and geopolitical environment also stresses the need for regulation and governance to achieve and maintain the right balance between open, networked systems, and security of closed environments. If nothing more than providing the forum for debate and discussion, Baird (2002) believed the role of the government is unique as a mediator and enforcer. The wild wild west mentality that suggests software coders set the laws to guide and restrict society's behavior are not in congruence with the views of the people. Baird's research indicated that society, by a margin on two-to-one, prefer government regulation of the Internet. In order to sustain its mediator role, the focus must shift to finding ways to make the government oversight and intervention speedy, agile and as technologically savvy as possible (Baird, 2002, p 18).

In addition to the government's role, Conner et al. (2003) suggested that companies should begin developing programs to comply with existing regulatory directions. Non compliance can result in a significant impact to the United States, private sector and governments. Shah, Mohammad, Zaighman, and Azia's (2009) banking industry case study research reaffirmed that information security is the predominant concern in the banking industry's quest for improved electronic governance. Nonetheless, banks are still worried that too much security, like multiple passwords and access controls, will drive customers away. If the basic controls are not in place, penalties include criminal, civil actions and privacy violations. Therefore, the charge to industry is to develop an information security governance framework that is balanced and that can be readily adopted.

It is commonly understood that the cost of security is not cheap and it is extremely difficult to show return on investment using standard models whether you are the government or commercial sector. Nonetheless, governing legislation in response to public concern has forced issuing legislation in such areas as accounting reform, investor protection, and personal health information. Discussions in Congress continue about the need to make vulnerability reporting by companies mandatory through either Congress or the Security and Exchange Commission (SEC). Despite decisions made in the best interest of society, unintended consequences of this type of governance can limit investment for advanced technologies, slow production and growth, and reduce the availability and accessibility of these services to citizens and consumers. Simonsson, Johnson, and Ekstedt (2010) stated that there is a direct correlation between information

technology governance maturity and performance so perhaps the legislation is necessary to motivate businesses to mature their governance processes and lead to better security performance.

Challenges that lie ahead involve the borderless nature of an Internet that can dilute the best governing rules (Conner, Noonan, & Holleyman, 2003). In order to legitimize the governance process developing countries and under represented parties must be consulted to ensure democratic accountability. With that accountability comes additional challenges because developing countries may lack sufficient financial and human resources, have poorly structured decision making arrangements, and not understand how technology can benefit them directly. Addressing these challenges is another reason that Baird (2002) felt broader groups like the World Trade Organization (WTO), International Monetary Fund, and the World Bank should be engaged to help plot the future path. The debate about global governance is essentially about participation, accountability, and transparency (Baird, 2002, p. 20).

After reviewing nearly 20 information security initiatives, Conner et al. (2003) summarized that what is needed is a governance framework that private industry can readily adopt but there is no one-size-fits-all solution. FISMA may be overly detailed for the private sector, but its principles can be applied to all organizations. Organizations can use these frameworks to articulate its goals, evaluate information security over time and determine the need for additional measures.

Non traditional bodies such as the Internet Cooperation for Assigned Names and Numbers (ICANN) are cited as a good example of how improved openness and

accountability can be managed through governance on a global scale. The openness it displays with various private and public interest groups gives ICANN its credibility. A global database of Internet domain users is an Internet governance success story of international proportions. Anyone requiring a domain name to interact on the Internet must be registered and provide their contact information. Mueller and Chango (2008) applauded the efforts of the United States in establishing the rules and managing this global governance initiative. As the Internet become more essential to every day life, governing institutions will be expected to step in and protect citizens from harm as innovation is embraced.

IT Governance Institute Perspective

The IT governance institute is a non profit, independent research firm that offers original and case study research to help enterprise leaders and boards of directors fulfill their IT governance responsibilities. The IT Governance Institute (ITGI) supported Pricewaterhouse Coopers in conducting a survey from May until August 2008 that looked at the four general topics: importance of IT, outcome of IT, IT accountability, and effectiveness of governance. More than 25 interviews were conducted in 22 countries where executives of large and small companies in a variety of industries were interviewed.

The purpose of the survey was to target top non IT executives and ascertain their opinions on IT's contributions to the business and the way their enterprises are governing IT. IT's contributions to efficiency and effectiveness were deemed more important than its innovation value. Organization culture was the most prevalent barrier preventing full

return from IT investments. Additionally, strong IT governance practices correlate positively with better IT outcome and the majority believed IT's performance was in line with expectations. In terms of the effectiveness of IT governance, operational performance is at the top of the list of IT subjects mentioned at board meetings. External advisors are the prime method used as a source of IT governance guidance by a large margin of 40 %. Based on this ITGI sponsored research, there appears to be strong indications that better IT governance practices lead to improved IT outcomes (Pricewaterhouse Coopers, 2008, p. 25).

Best Practice (ISO/IEC 17799) Perspective

The ISO/IEC 17799 is a standard that provided an information security framework that helps ensure business continuity, legal compliance, and gain competitive advantage (Saint-Germain, 2005, p. 60). Saint-Germain (2005) explained that each organization will have to select the specific controls for their own environment; however, the standard is a good launch point. The ISO/IEC 17799 standard is also the only one that requires organizations to undergo third party audits. The strength of the ISO/IEC 17799 standard is that it is more comprehensive and not solely focused on governance but also includes technical implementation guidance.

The standard is quite detailed and it is comprised of 10 security domains that address security compliance at various levels. There are 36 control objectives for each of the domains and 127 controls that specify the means for meeting the control objectives. The 10 security domains are: (a) Security Policy – management commitment demonstration, (b) Organizational Security – allocate security responsibility, (c) Asset

Classification and Control – proper levels of protection for critical or sensitive assets, (d) Personnel Security – reduce risk of errors through training, (e) Physical and Environmental Security – unauthorized access and damage, (f) Communications and Operations Management – ensure proper and secure use of information processing facilities, (g) Access Control – control access and detect unauthorized activities, (h) Systems Development and Maintenance – prevent loss, modification, or misuse of information, (i) Business Continuity Management – develop rapid reaction capability to failures or incidents, (j) Compliance - ensure all laws and regulations are respected.

In terms of implementation in various size organizations, Saint-Germaine (2005) suggested a structure driven from the top down. In small companies the ISO/IEC standard is a good foundation for information security management. Medium size companies can use the standard to develop information security policies, and large enterprises can use the standard to improve their security management systems. Saint-Germaine (2005) also explained that international proposals are beginning to require that organizations be ISO/IEC 17799 compliant. Although initial implementations were only in Europe and Asia, the standard has been largely adopted as the de facto international standard in many other countries: Japan, Netherlands, Spain, New Zealand, Iceland, Brazil etc. Compared to other best practices and compliance frameworks, ISO/IEC 17799 seems to be more comprehensive, focused on organizational and administrative issues, and mutually complementary to other frameworks.

Model Citizen Governance Vision

In the late 1990s the Government of Canada started an initiative to become recognized around the world as the "model user" of information technology. There were governance techniques that had to be changed to negotiate what Fraser (2007) called the changing relationships between nation, state, and citizens. Canada believed that not only was it important to provide strong leadership to move it toward a true information society, but also to be innovative in public service and become a model user. To realize this vision the government understood it had to overcome tensions between practices, procedures, rules, and constitutive relations among public institutions, organizations, businesses, and citizens. The government likened this adventure to the one experienced during the creation of the Internet. At that time, many characterized the Internet as the wild west or an electronics frontier that was ungovernable. The government was seen as desperately trying to keep pace with technological changes that were setting the pace of social progress.

Fraser (2007) showed that the role of the government is to "create favorable conditions for private enterprise and off-load public responsibility onto citizens in a discourse that emphasizes individualism and entrepreneurialism" (p. 203). In order to create these favorable conditions organizations must be open to new techniques of governance: new arrangements, organizational patters, forms of knowledge production. Conversely, some argue that these new forms of communication make regulatory strategies obsolete. The Canadian situation indicated a constant adjusting situation from the various pressures of what constituted a good consumer citizen. Catalyzing

developments in information technology implied the government would find new commercial applications and offer the private sector opportunities to add value and market government owned materials. This change also gave the government opportunities to develop more commercialization. Siber Systems (2007) pointed out that characterization of the Internet as integral to social progress veiled disparities in equity, access, and participation based on gender and class that had to be addressed. Autonomy became the experience of many users instead of personal freedom on the information highway. In a survey of 600 information technology professionals asked questions about passwords, the participants believed they have too many passwords to remember. This trend has wasted help desk technicians' time constantly resetting passwords, increased user frustration, and decreased security (Siber Systems, 2007).

Fraser (2007) noted the autonomous and frustrating feelings of users and adds that culture was also a prominent issue because subjects did not simply conform to governmental practices but tried to subtly change the procedures to fit their own ideas, values and beliefs. Conversely, entrepreneurship was advanced through this idea of developing global markets and improved trade relations. Because Canada focused on resource-sharing, global cultural diversity, international collaboration and economic prosperity their policy agenda was truly reflective of a model practice (Fraser, 2007).

Governance through Audits and Controls

Governance model precepts in information security espoused by Le Grand (2003) listed 10 areas where controls must be implemented effectively: accountability, awareness, ethics, multidisciplinary considerations, proportionality, integration,

timeliness, assessment, equity, and information sharing. Accountability is the management system put in place to ensure effective assignment of accountability. Awareness is another management challenge to ensure everyone buys in to the need for sound information security. Managers must provide guidelines that explain ethical and unethical behavior in using information systems. Leadership approaches must be multidisciplinary so everyone's interests are considered and balanced in policy descriptions. As the security controls are selected there must be some analysis applied in selecting specific controls to ensure proportionality. Grubb and Burke (2008) explained that banks have had a great deal of success in information security governance by ensuring their compliance and operational improvements are complimentary. In order to have effective security throughout managers must integrate security with overall policies.

Dodd (2005) pointed out that information system security must also be aligned to deliver upon the business strategy. Therefore, the policies and controls should be developed and selected to improve business operations. Failures are inevitable so timeliness measures must be put in place so the organization will not be endangered through operational impairment. The capability to continuously assess risks and manage them is also an essential capability. Addressing fairness and legality concerns ensure equity in information security measure selection and application. Information sharing with peers and government organizations give added credibility to organizations' information security programs. LeGrand (2003) stated that effective information security management and monitoring practices can be adopted and enforced by management or they will eventually be mandated by regulation (p. 56). Mathiasen (2008) suggested a

change in implementing and enforcing controls that seeks to understand how everyday people experience security. It is proposed that security designs should go beyond usability and secure behavior to create a secure experience for users. Existing systems are based on a military philosophy of need to know that enforces a hierarchy of control that does not work in general society.

Malcolm (2008) criticized the Internet Governance Forum (IGF) as only addressing issues in an ad hoc and isolated manner. For example, private negotiations, outside the IGF, have taken place on key issues affecting Internet public policies. On the issue of illegally sharing copyright material, Internet monitoring and filtering programs, and oversight of ICANN's discussions on a global secure domain name service (DNS) the IGF has not been involved. Privacy interests in the WHOIS service that identifies owners of Internet domains and setting policy for new top-level generic domain names is another major policy issue in which the IGF has been absent in addressing. The public policy issues of intellectual property, Internet filtering, and privacy are clearly responsibilities of the IGF that should be addressed in the multi stakeholder forum (Malcolm, 2008).

Although based on sound governance principles, the IGF can be improved to act as an open, multi stakeholder forum. Its discussions should carry normative influence, be reflected in the development of policy by both public and private organizations, through direct participation, or coordination of activities. Malcolm (2008) concluded that the weakness of the IGF is that it has not yet earned such authority within the Internet regime largely due to its structure.

Social Governance Experiences

Landell-Mills (2003) stated that the dramatic evolution of information technology has opened up a tremendous new potential for increasing governance to strengthen public accountability. Throughout history there has been a struggle in mankind where leaders' main ambition was to hold on to power and use it for their self-interests. Democracies are beginning to arise in more countries to help curb this struggle toward a belief in representing the interests of society. Sweeney (2007) supported Landell-Mills' thoughts about a new potential, but cautions that for electronic governance, trust between the people and government is still lacking. Although, society has demonstrated trust in technology it still is leery of policies enforced by the government. Perhaps this trust has not improved significantly, because governance remains a function of the political system.

Discussions have evolved to focus on improvements in the quality of public services, making the public agencies more accountable and transparent. Landell-Mills (2003) saw the key components of good governance as: "good public sector management with accountable public institutions, transparent policy-making and implementation, clarity, stability and fairness in the rule of law, and openness to the participation of affected citizens" (p. 357). The quality of governance determines whether a nation will advance rapidly or lag behind in the world and if accountability is lacking, the people will perceive the system as lacking legitimacy (Landell-Mills, 2003).

Summary

The observations of various researchers have helped shape the development of management and governing principles for an improved information security landscape. This section (Table 1) lists 41 themes extracted from research that describe many of the management and governance issues, approaches, and principles that can be applied by executives and managers in government and broader society. The first 22 themes reference specific management considerations, the next 9 are recognized contributions of the FISMA and the final 10 are governance principles. Prominent among these observations is the central idea that governance is essential and a primary focus should be on individuals in society as the root elemental factor that will derive the most effective and lasting benefit to continued innovation with minimal security risk.

Table 1

Security management and governance themes

Nbr	Theme descriptions	Literary source
1	Informed by past management theories like McGregor's theory X and Y, focus on the individual user's behavior.	Fraser, 2007
2	Important to be able to understand individual worker's behavior in response to implemented security controls.	Drucker, 2008
3	Study individual worker's behavioral responses to implemented security controls.	Drucker, 2008
4	Use observation and analysis of behavioral changes, but do not develop conclusive reasons…just use to broaden intellectual understanding.	Weber, 1962
5	Recognize changes in staff and line management relationships that affect a manager's ability to control human behavior before implementing security controls.	Hersey, Blanchard & Johnson, 1996 and McGregor, 1960
6	Diverse information sharing needs call for diversity in the types of controls that will be applied.	Mintzberg, 1989

table continues

Nbr	Theme descriptions	Literary source
7	Adjust to organizational management shift to a more legally defined construct, away from command and control, to comply with laws aimed at protecting the common good of society.	Conner, Noonan & Holleyman, 2003
8	Continue striving for balance between control, authority, and motivation as persuasion methods to achieve organizational goals and objectives.	Drucker, 2008
9	Recognize that human needs are not as important to today's knowledge worker.	McGregor, 1960
10	In order to have a knowledge environment, teach people how to learn.	Drucker, 2008
11	Prepare for a changing organizational landscape where knowledge is the key resource to be managed. Focus on more upward mobility opportunities, continual training, and changing demographics.	Fayol, 1987
12	Recognize that social impacts in businesses are coming from new innovations or technological improvements.	Mintzberg, 1989
13	Recognize and respond to social impacts that come from new innovations, controls, and technological improvements.	Mintzberg, 1989
14	Prepare to accept the ever increasing availability of information used to make decisions.	Fayol, 1987
15	Address people, processes and technology resources individually and in an integrated fashion to get the maximum benefit for the organization.	Drucker, 2008
16	Be willing to give up something to make room for new initiatives, work systematically to get new opportunities, use discipline in implementing ideas, tie innovation to business strategy.	Drucker, 2008
17	Stay focused on objectives because they are still seen as the guiding lights in a strategic plan.	Drucker, 2008
18	Prepare to respond to people's different ways of acting, thinking, and characterizing actions based upon access to unimagined information sources and types.	Edersheim, 2007 and Brown & Grant, 2005
19	Institute productivity controls keyed on working instead of the work itself because skill and knowledge is in the action rather than the act.	Hersey, Blanchard & Johnson, 1996
20	In developing new business ventures factor in the social impacts early on.	Hersey, Blanchard & Johnson, 1996

table continues

Nbr	Theme descriptions	Literary source
21	Be prepared and participate in discussions aimed at rationalizing the affects of controls on society through regulation of the profit oriented nature of business.	Hersey, Blanchard & Johnson, 1996
22	Avoid over quantification of control measures to make them better.	Hersey, Blanchard & Johnson, 1996
	Federal Information Security Management Act Principles	
23	Federal Information Security Management Act (FISMA) of 2002 has standardized the methodology used to provide a consistently repeatable information assurance program for use throughout the federal government.	Newell, 2007
24	Provides minimum set of controls specified in policy publication. Improves management oversight by directing appointment of key leaders like the chief information officer.	FISMA, 2002
25	Dictates use of commercial products to institute standardization and reduce duplicative expenses.	FISMA, 2002
26	Directly assigns specific and detailed responsibilities to individual government agency leaders.	FISMA, 2002
27	Avoid a one size fits all implementation approach that ignores the constraints placed on smaller segments of an organization or society.	Newell, 2007
28	Implement controls incrementally so cultural change impacts are not so dramatic.	Newell, 2007
29	Ensure information sharing and collaboration are not hampered by over protection (classification) of information.	Hoover, 2009a
30	Pay attention to process, data, and technology standardization and simplification techniques that can be as effective in achieving organizational goals as controls.	Volonino, Gessner, & Kermis, 2004
31	Establish a governance framework that is responsive to regulatory guidelines, treats information technology as both a governance and technology issue.	Conner, Noonan & Holleyman, 2003
	Governance Principles	
32	Lack of balance and transparency in government power sharing with experts in the IT community, business sector and non profit organizations.	Baird, 2002

table continues

Nbr	Theme descriptions	Literary source
33	Open and closed network systems are not sufficiently regulated, through governance, to address new economic and geopolitical issues.	Baird, 2002
34	Government is not taking the position as a mediator or enforcer to ensure a debate forum is established.	Baird, 2002
35	Legitimization of governance processes is weakened because smaller sectors of society (e.g. non profits) are under represented in collaborative discussion forums.	Baird, 2002
36	Dramatic nature of cultural impacts on the success of governance policies is not recognized and it prevents achieving intended objectives.	Pricewaterhouse Coopers, 2008 and Fraser, 2007
37	The positive correlation between strong governance and better IT outcomes/results is under estimated.	Pricewaterhouse Coopers, 2008
38	Organizations are not open to new techniques of governance: new arrangements, organizational patterns, and forms of knowledge production.	Fraser, 2007
39	Governing policies are not seen as creating favorable conditions for private enterprises and placing responsibility with citizens/employees to emphasize individualism and entrepreneurialism.	Fraser, 2007
40	Lack of trust people place in electronic government is still very low.	Sweeney, 2007
41	Weak public sector management with accountable institutions, lack of policy-making transparency, perceived unfairness in the rule of law, and lack of openness to citizen/employee participation detract from the effectiveness of governance policies.	Landell-Mills, 2003

Chapter 3 provides detailed information that describes the overall research methodology that was chosen. The specific type of research design will be explained, the nature of the population is described, the type of sampling procedure used is explained, the data gathering method is described, the particular method for presenting and analyzing data is explained, and ethical consideration are assessed.

Chapter 3: Research Method

Introduction

This chapter presents the methods used to address the core research questions posed in this case study analysis. The purpose of the study was to discover central themes that can help shape the future development of information security governance policies, controls, and practices. Knowledge and understanding of these themes can help manage individual and societal behavior to reduce security vulnerabilities (Landell-Mills, 2003). This research method was designed as a case study to gain the perspective of military managers and leaders who are charged to follow the prescriptive guidelines of federal legislation. The military was a proper target audience because it places more emphasis on information security than any other sector of society (Hoover, 2009b). The security threats are so severe that congressional legislation was passed to direct certain management and governance procedures be followed.

As a first step in determining the viability of using a case study methodological process, extensive literary research is conducted to gather information which answers key research questions. Yin (2009) pointed out that the literature review leads to developing sharper and more insightful questions. The literature review can serve as a means to an end and help shape the general research questions. After analysis, integration, and synthesis of the information, key themes are detailed. The themes are then used to develop and compile survey or interview questions for the military case study. The case study survey responses were

analyzed to validate literary research themes and form the basis for future theories, frameworks, research or general management application. Particular focus is on the concept that information security governance is a pacing factor for innovation. New technological advances are restricted due to the inherent security risks they pose (Grubb & Burke, 2008). The chapter is organized to provide an overview of the research design, population, sampling procedures, measurement, data collection processes, data analyses, and ethical guidelines.

Description of the Research Design

The proposed research design for this study is qualitative. Singleton and Straits (2005) explained that research is undertaken for basically three reasons: (a) explore a phenomenon, (b) describe a situation, or (c) test relationships or explanatory study. In determining what particular research design will be used it is prudent to review the implications of these three functions. Exploratory studies are generally taken when little is known about a subject because it may be new or unusual (Singleton & Straits, 2005). Singleton and Straits also state that this type of research is difficult because there are no clearly defined dependent and independent variables identified. A descriptive design is more structured and focused on fact finding. Singleton and Straits stated that the descriptive design is focused on few dimensions that have well-defined entities and the entities can be measured through a systematic process with detailed numerical descriptions.

Testing relationships is the third purpose for conducting research. These studies are often called explanatory because they seek answers to problems and hypotheses (Yin,

2009). Yin stated that it is the scope of the description that distinguishes explanatory from descriptive research. If research is purely descriptive it seeks to describe information about isolated variables instead of looking at relationships between variables. Yin explained that how and why questions are more explanatory because they deal with operational links needing to be traced over time instead of just frequencies or incidence (p. 9). Before beginning the research process it is essential to anticipate all the steps throughout the entire process (Singleton & Straits, 2005, p. 69).

Creswell (2007) asserted that the general characteristics of qualitative research place the observer in the world being studied so real world practices can be more easily interpreted (p. 36). The world is transformed through definitions of itself in field notes, interviews, and conversations. Creswell also explained that qualitative research begins with assumptions, a world view, and the use of a theoretical lens to study the research problem. When conducting qualitative research it is important for the researcher to collect data in a natural setting. Multiple forms of data like interviews, observations, and documents should be collected. A theoretical lens should be used to view the study from a social, historical or political perspective. Viewing the study in this manner helps visualize patterns, categories, or themes for subsequent interpretation and reporting on the views of the participants (Creswell, 2007, p. 37).

The type of qualitative research design method proposed for this study was a case study. According to Creswell (2007), case study research involved the study of an issue that is explored through one or more cases within a bounded system (p. 73). The case study approach is familiar in social science research, particularly in the psychology,

medicine, and law fields. The types of case studies are distinguished largely by the size, bounded cases, entire programs, or activities (Creswell, 2007).

Creswell (2007) and Yin (2009) indicated that the qualitative research design is appropriate for this research study because it supports research that is focused on fact finding and describing a particular situation. This research report described the current information security governance situation in the federal government based on founding federal legislation, managerial theories, and literary governance research. The purpose of the study was to uncover facts that can be shaped into central themes that can be used to develop and further refine present theories, concepts, frameworks, and models. The characteristics of qualitative research also support the method of research needed to gather background information, analyze it and make interpretations (Singleton & Straits, 2005). The case study methodology is suited for this research approach because the type of research questions posed are how and why questions, it does not seek to exercise control over behavioral elements, and the focus is on contemporary issues instead of historical events (Yin, 2009).

The study of information security governance was bounded within the context of the federal government (inclusive of the department of defense); however, described and analyzed from internal and external perspectives to voice similar and differing views. The intent of the study was to design an explanatory case study because the focus was on a single information security governance case that is experiencing an unusual, difficult or unique situation. The case study allowed bringing forth the voices of those individuals that are directly involved in the situation, as well as, the views of professionals who have

studied and analyzed the situation. The qualitative research design and case study methodology supported the central objectives of the research approach of identifying issues, synthesizing them, and finding the common themes that can be used to further research in this area.

A quantitative research design with another analysis methodology could be used; however, the purpose of conducting research to discover central themes is best suited with qualitative analysis (Leedy & Ormrod, 2005). The intent was not to identify independent and dependent variables that can be used in comparative analysis but find descriptive information and then look for common trends in thinking or approaches. A mixed mode research method could have been selected but this approach would extend the scope of the research study and could diminish the focus on discovery and describing to comparative analysis. More extensive comparative analysis, from a quantitative perspective, should be a follow on research study after this effort uncovers and validates central themes and concepts.

Target Population

The ICAF mission is to prepare selected military and civilians for strategic leadership and success in developing our national security strategy and in evaluating, marshalling, and managing resources in the execution of that strategy (Industrial College of the Armed Forces, n.d.). The nature of the population for this study is a department of defense university that teaches national security resource strategy. The university students are senior level military officers and civilians that have been chosen through a competitive selection process. After graduation the students will be sent to key leadership

positions throughout the department of defense and federal agencies. Each student earns a masters degree after successfully completing the eleven month program of study. The students will normally all have masters degrees and have worked in the defense department for between 13 to 16 years (Industrial College of the Armed Forces, n.d.). The age of the students is usually from mid to late 40s and the percentage of females and ethnic makeup is factored into selections in order to enrich the learning experience and represent the demographics of the department of defense in general. Industrial College of the Armed Forces (n.d.) indicated that fifty eight percent of the student body is composed of military representatives from the land, sea and air services, 32 % from the departments of defense and state, 10 % other federal agencies, 8 % international military officers, and 2 % from the private sector. This diverse mixture provides a good target population to represent the larger department of defense.

The ICAF faculty is composed of military officers from all four services and civilian academics who are experts in their fields. Military faculty hold the rank of colonel or captain and are highly qualified subject matter experts with specialized experience (Industrial College of the Armed Forces, n.d.). The civilian faculty, typically hold doctorates or the equivalent, include full-time academicians, state department representatives, and visiting professors from selected federal agencies. A sample was drawn from this population of 150 permanent students who attended the industrial college of the armed forces class of 2010. Correspondence students and those attending other shorter term courses were not part of the research population because they do not share the same cultural experience as the permanent students in the 11 month program.

Members of the faculty were not included in the sample population or other employees of the university. Only students that were enrolled in the university's permanent program were considered. Alumni graduates were also excluded.

Sampling Procedure

The selected sampling frame was 150 permanent residence students. Sampling this population ensured a strong representation of the population and provided evidence for inferences about the larger defense department population. The characteristics and demographics of the sample were those outlined in the university's student selection processes. The university strives to select students from various military services, agencies, departments with varied demographic backgrounds (Industrial College of the Armed Forces, n.d.). The makeup of the student population was heterogeneous because they came from different military services and agencies throughout the federal government, had varied technical backgrounds, and professional experiences. Precision is largely a factor of population size so as long as the selected population is large the proportion selected is not as important (Singleton & Straits, 2005). Fifty percent of the sampling frame was the objective to ensure a fair and equitable representation. At 95% certainty (confidence) the suggested sample size is 109, so 150 students would provide the required number of students to achieve a high confidence level (Aczel & Sounderpandian, 2009).

The analysis approach for this study was purposive non probability sampling because the researcher's expert judgment is being applied to select representative or typical units of the population. Purposive sampling starts with a purpose in mind and the

sample is thus selected to include people of interest and exclude those who do not suit the purpose (Leedy & Ormrod, 2005). This type of sampling is prone to bias and error because it does not depend on random selection or probability theories. The university selected for study is a sub representation of leaders throughout the federal government population. The students came from all military services, defense agencies, and were typical of defense department employee demographics so this helps balance any random selection bias. I had knowledge of the population so expert judgment can be applied to overcome weaknesses in making informed selections or analysis decisions (Singleton & Straits, 2005).

The sampling design was purposive to allow flexibility in sample selection and application of judgment. Selecting the university students eliminated the need for a large number of research man hours to help collect information. The number of breakdowns planned were minimal because the focus was on discovering and validating common themes from the views expressed by other researchers and espoused in founding legislation and governing literature. As a basic break down, it may be informative to view the collected information by military service (Air Force, Army, Navy, Marine Corps, Coast Guard), civilians, and international students).

The unit of analysis was federal government managers attending the industrial college of the armed forces. The research design was not focused on relationships but discovery of views from this population based on specified research themes, questions, and assessments. Sampling was conducted to establish broad generalizations; however, this research study did not seek to generalize but identify common and central elements

of thought on the subject of information security governance. In terms of measurement precision, it was not as important in this study because the objective was to discover interesting patterns that can be used to generate hypothesis or themes for later study, analysis, or implementation (Leedy & Ormrod, 2005).

Instrumentation

The primary data gathering tool was a survey or specifically a self administered questionnaire that will be given to a select number of students. The questionnaire was developed from the common themes that are uncovered after synthesizing information from the literature research material. The survey question responses were placed on a Likert scale so respondents can select the degree of their agreement or disagreement with the research theme questions. Likert scales represent a set of attitude statements where each item of interest is judged and involves the use of a standardized set of responses (Singleton & Straits, 2005). Each question was worded to elicit a measured response so not only will the respondent's agreement be determined but the relative strength of their belief as well.

The research material included peer reviewed research, government accountability office reports, and founding legislation and policies. Performing a critical review and analysis of this information yielded key themes, ideas, and opinions used to design questions. The questions provided the focus needed to gather further opinions and views from members of the federal government population attending the industrial college of the armed forces. The experts and professionals in the government helped validate the themes that are prevalent in literary research and operationalize them to

become theoretical tenants or principles for a future information security governance framework or theory.

If further analysis or validation of the themes was necessary due to discrepant cases, the interview would be reissued to a smaller subset of the target population to provide clarification. A request to the Institutional Review Board to conduct further interviews from other government officials may be submitted to provide corroborating information. The officials may be other students at the university or experts in the field from different government agencies. The objectives would be to ask specific questions that have been written beforehand and ask them in the same order to all respondents. Singleton and Straits (2005) pointed out that when the research purpose is not to derive facts or precise quantitative descriptions but to understand the respondents' experiences, unstructured interviews can be helpful. This approach also allows flexibility in developing a hypothesis or theory. Although not required, interviews would have been conducted via telephone or face to face depending on the availability of respondents. Each method has its own set of pros and cons but can help reduce various types of errors like sampling and measurement errors (Leedy & Ormrod, 2005).

Major disadvantages of surveys are their use in explanatory research, criteria for inferring cause and effect relationships can not be established, and the criterion of directionality (cause must influence its effect) become largely matters of interpretation. The surveys are usually highly standardized so flexibility in gathering information can be restricted (Singleton & Straits, 2005). Surveys are also susceptible to reactivity which can introduce systematic measurement error. Errors can also result from respondent's lack of

truthfulness, misunderstandings of questions, or inability to recall past events accurately (Yin, 2009). As much as possible, these factors were addressed in the design of the survey instrument and implementation process.

Close ended questions were used because the purpose of the surveys was to discover consensus among several themes based on extensive literary research. The closed ended questions helped keep the respondents focused on providing their ideas about specified themes of interest. Precautions were taken to avoid structuring responses or inserting undue biases by following instrumentation preparation guidelines expressed by Singleton and Straits (2005) such as preparing questions, response format, and instructions. Pretesting of the surveys was performed via a pilot to ensure respondents understood the questions and help ease the burden of analyzing responses later. Pretests helped address issues that could arise concerning validity and reliability.

In order to overcome validity concerns, the survey form was organized, all questions were reviewed to ensure they fall within the research area, measures of the same category were reviewed to ensure they are comparable, and an effort made to ensure the survey did what it was intended. In terms of survey design Leedy and Ormrod (2005) explained it must also ensure effective two way communications, help respondents recall information, and keep them interested in the topic. As an additional technique to ensure validity and reliability, the research themes and research questions were analyzed using a matrix to assess how they are related and ensure all the themes were covered in the instrument.

Data Collection Procedures

Questionnaires were used to collect data from the university students. The questions used on the survey questionnaire were developed from the key themes that were summarized from the literature review and analysis. After institutional review board (IRB) approval, an introductory and consent letter, which included an internet link to the questionnaire, was sent to each student's college e-mail address. The introductory letter explained the purpose of the research study, explained how to access the internet site and complete the survey, stressed that it is anonymous and provided contact information if there were problems or questions.

The survey was administered anonymously from the Survey Monkey web site. Survey Monkey allowed preparation, design, and administration of the survey online. The students were able to access and complete the survey via the internet. Their responses were stored in a password protected file for collection by the researcher. The survey services of Survey Monkey also included the ability to monitor the survey completion status in real time. After the established survey completion time frame of one month the survey was closed and the data downloaded for analysis.

Data Analysis Procedures

Case study data analysis is the process of developing detailed descriptions of the case and its setting (Creswell, 2007, p. 163). There are four primary forms of data and interpretation in case study research: categorical aggregation, direct interpretation, and naturalistic generalizations (Creswell, 2007). In categorical aggregation it is the role of the researcher to look for a collection of instances from data so issue relevant meanings

can be found. Direct interpretation is where a single instance is looked at and from it the researcher looks for meaning. Creswell (2007) explained that this is simply pulling the data apart and putting it back together again in more meaningful ways. Patterns are also established and any correspondence between different research questions or themes is revealed. Naturalistic generalizations are developed from data analysis that people can learn from the case or apply to a population of cases. Summarizing these approaches in a description of the case can also be effective in drawing the reader's attention to key themes and how they compare and contrast with other research elements.

This research study presented data in narrative sentences or paragraphs that succinctly described the consensus view based on the survey results. The themes were placed into categories as they relate to the specified research questions and key study areas of managerial behavior theory, governance and federal information security management act policies. As categorical analysis was performed, the objective was for the survey responses to serve as the tenants of a framework that provides managers guidelines to follow in establishing and enforcing management and governance principles for information security. Prioritization of the tenants was not critical because each organization has to make that assessment based upon its unique business area. However, this study indicates which principles are essential to be considered in identifying leading managerial or governing policies.

Statistical analysis was not used for this study because the focus was on discovery and synthesis of views rather than comparative analysis. Descriptive statistical charts and graphs are used to study, analyze, and present the raw data results of information

obtained from the survey. Singleton and Straits (2005) explained that verifying qualitative data is where the researcher explains and clarifies any biases at the beginning of the study (p. 208). The research explained any past experiences, biases, prejudices, and orientations that may affect expressed views. Using this approach, readers will clearly understand the perspective introduced by the researcher and therefore be able to better evaluate and assess the validity of the study results.

Ethical Protection Measures

Leedy and Ormrod (2005) explained that ethical issues generally fall into four main categories: protection from harm, informed consent, right to privacy, and honesty with professional colleagues. Following Walden University's IRB application process ensured adequate measures were taken throughout the research process to preclude ethical conflicts. Assessments of any undue psychological, embarrassment, or stress were considered to ensure measures were in place to protect the respondents from harm. Participation in research was strictly voluntary and all participants were asked to acknowledge implicit consent criteria beforehand. The nature and quality of participants' performance or responses was kept strictly confidential. All research findings were reported in a complete and honest manner so as not to misrepresent or mislead anyone about the nature of the study.

Ethical protection measures were assessed and implemented through completion of a detailed IRB application (number 06-17-10-0385603) process before any research data were collected. The survey results were framed to ensure the study was bounded and central objectives followed. The data collection methodology ensured trustworthiness by

keeping the information strictly confidential and requesting acknowledgement of implicit consent. Concluding discussion and recommendations were aligned with the theoretical base for the research and linked to the three prime research questions. Analysis of patterns in the research themes and survey results were presented logically and void of personal experience bias.

Chapter 4: Results

Introduction

The purpose of the study was to discover ways management and governance practices in the federal government could be improved in response to information technology security challenges. The research method yielded information similar to expectations and no major adjustments in planning were required. Central themes were uncovered from the literary research that were used to design survey questions for a questionnaire that was given to a representative sample of federal government employees. The questionnaire elicited the views and voices of employees that could then be used to analyze and correlate responses to the basic research questions.

1. How can management practices be improved in the federal government sector of society to respond to current and emerging information technology security issues?

2. How has the federal information security management act contributed to improving IT security governance and management in the federal government?

3. Why are IT security governance practices not more effective in responding to current and emerging IT security issues?.

This chapter presents the results of the analyses that were conducted to address the major research questions of the research study. The initial section of this chapter explains how the results of the pilot study were developed before the main data collection procedures were implemented. The next section presents descriptive statistics for the

sample of federal government professionals who participated in the research study. As Yin (2009) suggested the preferred data analysis research strategy is to follow those theoretical propositions that led to the case study. The main body of this chapter addresses, in turn, analyzed and correlated responses to the three basic research questions used to frame the overall research study.

Pilot Study

A pilot study was constructed and disseminated to five federal government professionals to determine the effectiveness and understanding of the survey questions, feasibility and effectiveness of logistical procedure, and the approximate time required for answering the survey. The pilot survey participants were current employees with a large department of defense agency. The average time to complete the 41 question survey was about 20-30 minutes; however, several participants completed it over 2-3 days. Each respondent reported that they understood the questions and had no difficulty following the survey access instructions. The first respondent encountered an access problem because he was trying to use a login and password; however, the automated survey did not require it. A password required control setting was incorrectly selected. The pilot study provided an opportunity to learn the survey monkey tool's capabilities and plan a method for completing data analysis using various charts and software data filtering functions.

Methodology

The qualitative research design and case study methodology was appropriate for this study because it supported focusing on fact finding and describing a particular

situation. The design and methodology chosen helped uncover facts for shaping central themes that were later used to analyze survey data that has the potential to help refine future theories, concepts, frameworks, and models. The study was properly bounded within the context of the federal government by sampling employees attending a department of defense university. The central objectives of the research approach were followed to identify issues, synthesize information, and discover common themes.

In terms of trustworthiness of the data that were collected, the research design and methodology was selected to reduce any concerns in this area. A rigorous and thorough IRB examination process was followed to ensure trustworthiness concerns were addressed appropriately before starting the research. The IRB process ensured adequate measures were taken throughout the research process to preclude ethical conflicts. Assessments of undue psychological influence, embarrassment, or stress were also considered and participation was stressed as entirely voluntary.

Implicit consent acknowledgement was received from each respondent and a promise made to keep responses strictly confidential. An introductory letter was developed and given to each survey respondent to explain the purpose of the research study, survey was administered over the internet in an anonymous manner, and university IRB and mentor contact information was provided to respondents in case there were questions. The anonymous data were collected and stored securely. The data in no way specifically identify any of the respondents.

Data Analysis

Direct interpretative research and categorical analysis was used to look at each response and assess the meaning relative to the developed literary themes and theoretical research findings prepared in chapter 2. The intent was to find patterns and any relative correspondence between questions, themes, and theory. Creswell (2007) explained that qualitative data analysis consists largely of preparing and organizing, reducing the data to themes, and finally representing the data in tables or discussions. Correlation analysis, pie charts, line and bar graphs were used to analyze and report responses. The Survey Monkey software was used to perform data correlation and analysis. The survey was administered anonymously to 100 students via e-mail notification by an official from the Industrial College of the Armed Forces. Sixty-two out of 100 students completed the survey for a completion percentage of 62%; 37 answered all 41 questions. The following section describes the Information System Security Management and Governance Survey Results – Questions 2 thru 22.

Information System Security Management and Governance

This section's narrative and table 2 summarize an aggregation of the responses noted as important and very important from questions 2 – 22 on the survey questionnaire at Appendix A.

Table 2

Security management and governance responses

Question	Percent	Response (Important – Very Important)
2	91.7%	Assess employee behavior after implementing security controls
3	83.3%	Observe and analyze behavioral changes
4	36.6%	Line & staff management changes affect security effectiveness
5	85.7%	Need differing levels/degrees of security controls
6	76.4%	Important to develop legal constructs
7	82.4%	Instill command and control constructs to ensure compliance
8	75%	Balance use of control, authority and motivation
9	57.1%	Recognize human needs
10	51.4%	Have programs focused on learning vice factual teaching
11	80%	Establish knowledge environment
12	40%	Knowledge is the key resource to be managed
13	37.1%	IT innovations lead to social problems
14	48.6%	Respond to social concerns resulting from IT innovations
15	91%	Establish methods to manage increasing amount of information
16	94.3%	Address people, process and technology resources in policies
17	68.6%	Terminate existing projects to have resources for new initiatives
18	94.3%	Tie innovative ideas to business strategies
19	97.2%	Have objectives to guide strategic planning
20	54.3%	Respond to differing views, thinking and characterizations
21	80%	Factor in social impacts early when innovating
22	74.3%	Include employees in information security discussions

For question 2, a majority of respondents (91.7%) believed that it is important to assess an employee's behavior after putting security controls in place. For question 3, 83.3% of the respondents stated it is important to observe and analyze behavioral changes in order to understand how changes affect user's behavior while 3% answered that is not important. For question 4, 36.1% of the respondents believed that the changes in line and staff management relationships have a moderate affect on the manager's ability to implement security controls. 43.7% believed the line and staff changes would have a moderate to extremely high affect on managers. For question 5, 85.7% stated it is important to have different levels or degrees of controls to secure information sharing sessions.

For question 6, 76.4% stated it important to develop legal constructs for managers to ensure information security laws are understood and followed; 2.9% believe it not important. For question 7, 82.4% stated it is important to have command and control constructs in place to direct managers to comply with information security laws and policies. For question 8, 75% answered that it is of high to extremely high importance to balance control, authority and motivation in persuading employees to follow information security guidelines; 2.8% thought it was of low importance. For question 9, 57.1% stated it is important to recognize human needs in order to improve information security from an organizational perspective; 28.6% stated it was very important. For question 10, 51.4% believed it important to have programs focused on teaching people how to learn instead of teaching specific facts or instructions; 22.9% rated it very important. For question 11, 80% stated it was important to have a knowledge environment because of

the widespread use of information technology; 14.3% were neutral and 5.7% believed it somewhat important.

For question 12, 40% of the respondents indicated that, to a high degree, knowledge has become the key resource to be managed; 28.6% rated it extremely high and 28.6% rated it average. For question 13, the degree to which information technology innovations or improvements are causes for social problems was rated as low by 37.1% and average by 31.4%. For question 14, 48.6% believe it important to respond to social concerns discovered after new information technology has been implemented; 34% were neutral. For question 15, 91% of the respondents stated it important to have methods and procedures in place that explain how to manage the increasing amount of information; 8.6% were neutral.

For question 16, 94.3% stated it is important to address people, process and technology resources in policies in order to get the most benefit; 5.7% were neutral. For question 17, 68.6% stated it important to give up or terminate existing programs or projects in order to have resources for new initiatives; 25.7% were neutral. For question 18, 94.3% believed it important to have innovation initiatives tied to the business strategy; 5.7% were neutral. For question 19, 97.2% stated it important to have objectives that guide strategic planning; 2.9% were neutral. For question 20, 54.3% stated it important to respond to the differing views, thinking, and characterization of actions given access to so many different information types and sources; 11.4% stated it somewhat important. For question 21, 80% stated it important to factor in social impacts early when developing new business ventures; 11.4% were neutral. For question 22,

74.3% stated it important for employees to be included in information security manager discussions aimed at rationalizing the affects of information security controls; 14.3% were neutral. The next section provides correlative analysis information focused primarily on those responses which received at least 60% affirmation.

Information System Security Management and Governance Theme Correlation

At table 3, themes 1, 2, 14, 15, 20, and 21 have a strong positive affirmation of the positions developed from literary research because the percentage of responses to the specific survey questions were above 60%. Theme 3, 5 and 12 reflect a low affirmation for the literary research position with percentages from 36.1 to 38.2%. In all the remaining themes the affirmation is positive because a larger percentage of the responses supported the theme statement.

Table 3

Information systems security management and governance themes

Nbr	Theme Descriptions	Survey Ratings
1	Informed by past management theories like McGregor's theory X and Y, focus on the individual user's behavior.	63.9% - Important
2	Important to be able to understand individual worker's behavior in response to implemented security controls.	63.9%- Important
3	Study individual worker's behavioral responses to implemented security controls.	36.1% Important
4	Use observation and analysis of behavioral changes, but do not develop conclusive reasons…just use to broaden intellectual understanding.	48.6% - Important
5	Recognize changes in staff and line management relationships that affect a manager's ability to control human behavior before implementing security controls.	38.2% - Important
6	Diverse information sharing needs call for diversity in the types of controls that will be applied.	47.1% - Important
7	Adjust to organizational management shift to a more legally defined construct, away from command and control, to comply with laws aimed at protecting the common good of society.	52.8% - High degree

table continues

Nbr	Theme Descriptions	Survey Ratings
8	Continue striving for balance between control, authority, and motivation as persuasion methods to achieve organizational goals and objectives.	57.1% - Important
9	Recognize that human needs are not as important to today's knowledge worker.	51.4% - Important
10	In order to have a knowledge environment, teach people how to learn.	42.9% - Important
11	Prepare for a changing organizational landscape where knowledge is the key resource to be managed. Focus on more upward mobility opportunities, continual training, and changing demographics.	40% - High
12	Recognize that social impacts in businesses are coming from new innovations or technological improvements.	37.1% - Low degree
13	Recognize and respond to social impacts that come from new innovations, controls, and technological improvements.	48.6% - Important
14	Prepare to accept the ever increasing availability of information used to make decisions.	77.1% - Important
15	Address people, processes and technology resources individually and in an integrated fashion to get the maximum benefit for the organization.	85.7% - Important
16	Be willing to give up something to make room for new initiatives, work systematically to get new opportunities, use discipline in implementing ideas, tie innovation to business strategy.	48.6% - Important
17	Stay focused on objectives because they are still seen as the guiding lights in a strategic plan.	51.4% - Important
18	Prepare to respond to people's different ways of acting, thinking, and characterizing actions based upon access to unimagined information sources and types.	54.3% - Very Important
19	Institute productivity controls keyed on working instead of the work itself because skill and knowledge is in the action rather than the act.	54.3% - Important
20	In developing new business ventures factor in the social impacts early on.	80% - Important
21	Be prepared and participate in discussions aimed at rationalizing the affects of controls on society through regulation of the profit oriented nature of business.	74.3% - Important

Survey Results Assessment of Deviations

Figures 4-10 identify the survey results of the various themes that were developed from the literary research material. There appears to be general agreement with the research statements in most cases: (a) assessing individual user behavior, (b) observing and analyzing behavioral changes, (c) impact of staff and line changes on implementing security controls, (d) managing the increase in information, (e) addressing people,

process, technology, concerns in policies, (f) innovation social impacts, (g) and rationalizing the affects of controls on society. There was a high level of agreement with the need to stay informed by past management theories like McGregor's theory X and Y and focus on the individual user's behavior.

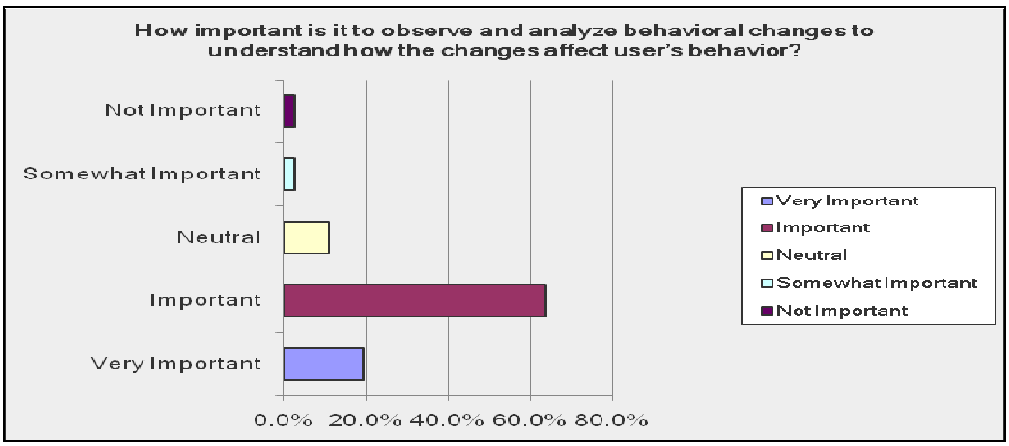

Figure 4. Individual user behavior

High level of agreement with the importance of being able to understand how changes affect individual behavior.

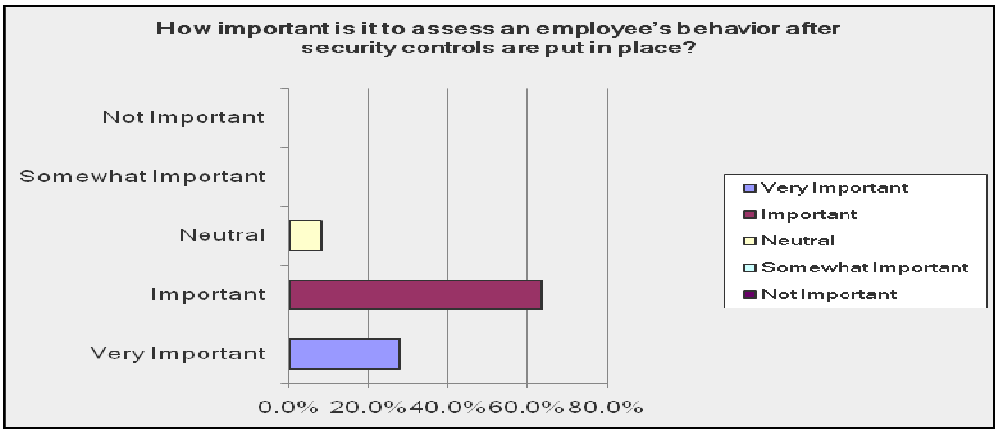

Figure 5. Observing behavioral changes

High level of agreement with the importance of being able to understand individual worker's behavior in response to implemented security controls.

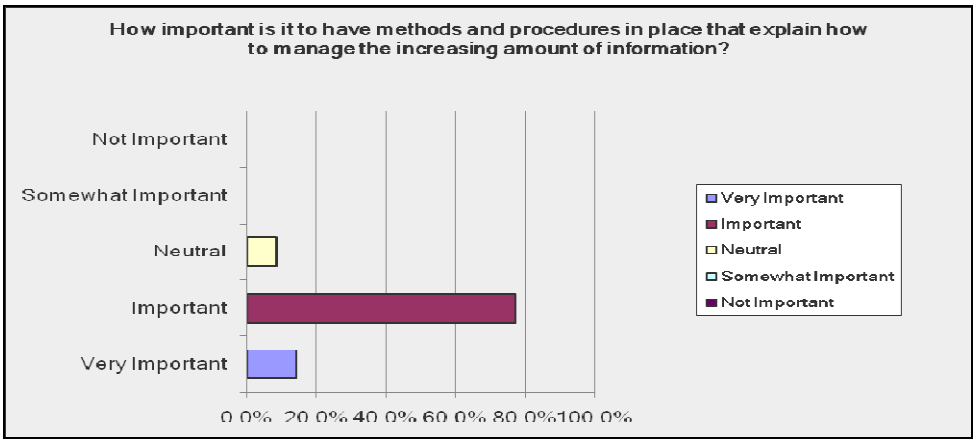

Figure 6. Manage increase in information

High level of affirmation of preparing to accept the ever increasing availability of information used to make decisions.

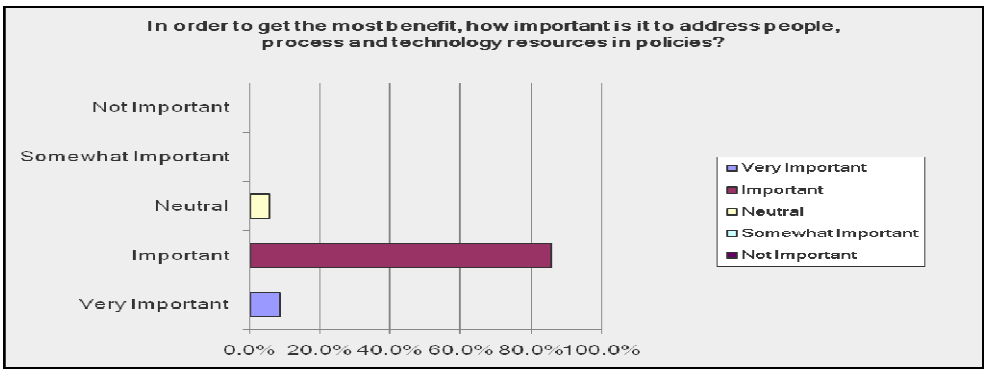

Figure 7. People, process, and technology

High level of affirmation to address people, processes and technology resources individually and in an integrated fashion to get the maximum benefit for the organization.

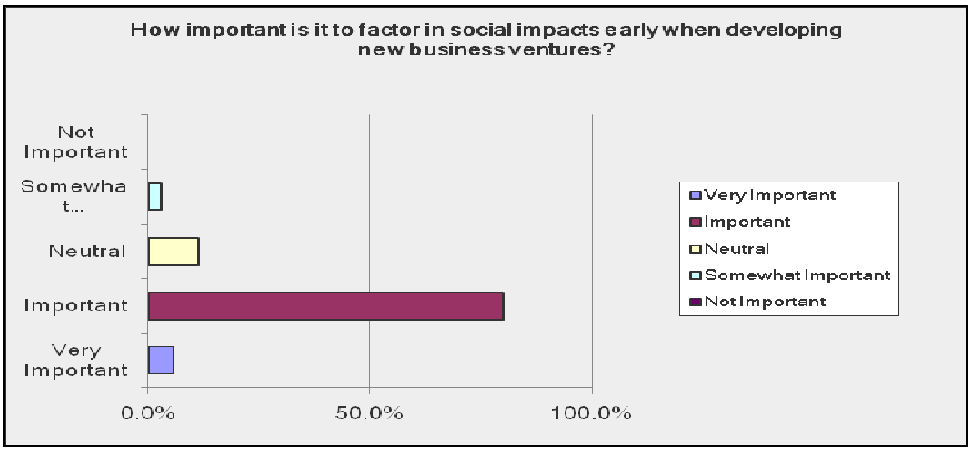

Figure 8. Innovation social impacts

High level of affirmation in factoring in the social impacts early when developing new business ventures.

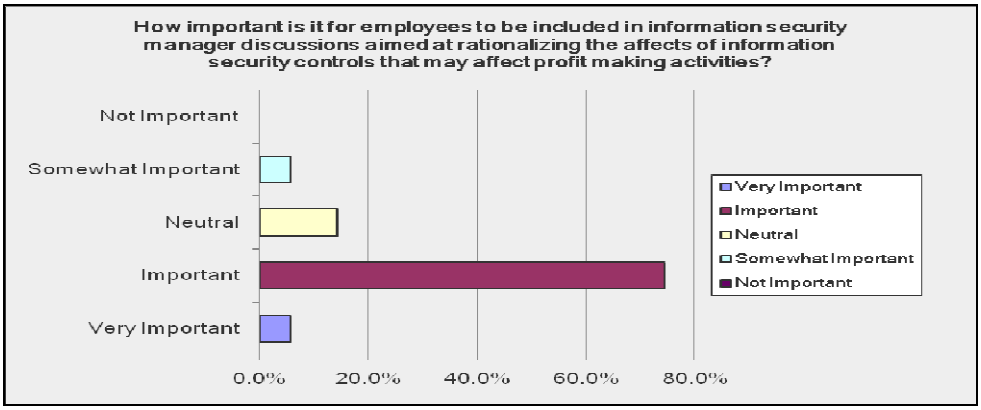

Figure 9. Information security control discussions

High level of agreement in being prepared and participating in discussions aimed at rationalizing the affects of controls on society through regulation of the profit oriented nature of business.

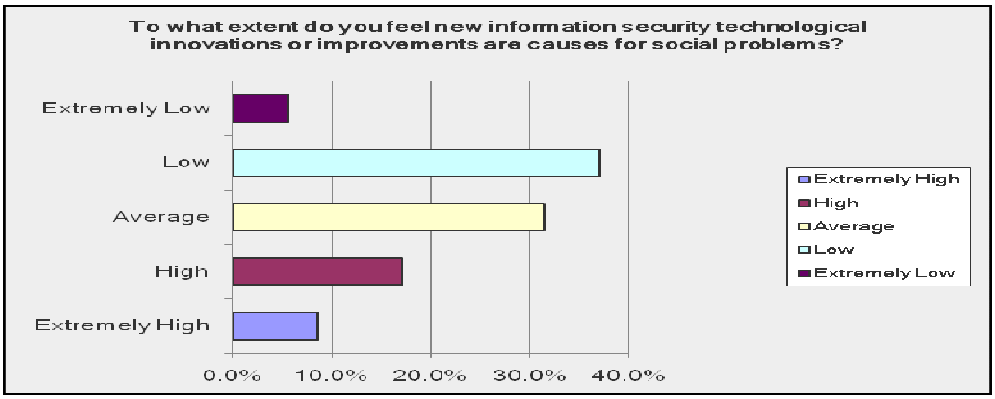

Figure 10. Social concerns

A deviation is noted in Figures 10 in the areas where innovations or improvements have been causes for social problems. Survey respondents did not see major causes of social problems.

Federal Information Security Management Act Principles

Correlative analysis of responses related to security principles and standards are explored in this section. The narrative and table 4 summarize the responses received from questions 23 - 31 on the survey questionnaire at Appendix A.

Table 4

FISMA responses

Question	Percent	Response (Important – Very Important)
23	65.2%	FISMA affect in helping standardize methodologies was average
24	50%	Important to appoint a chief information officer
25	45.8%	Direct use of commercial product for standardization
26	70.8%	Assign detailed and specific information security responsibilities
27	52.2%	On average FISMA does not ignore constraints to small segments
28	45.8%	Incrementally implement controls to lessen cultural impacts
29	41.7%	Important to classify information for sharing protection
30	33.3%	On average over-classification does not hamper sharing
31	45.8%	Standardization of processes support achieving security goals

For question 23, 65.2% of the respondents believe the degree that the federal information security management act of 2002 has standardized the methodology used to provide consistency in the federal government is average; 26.1% rated it as high. For question 24, 50% stated it important to appoint a chief information officer and assign the person responsibility for information security management; 20.8% were neutral and 16.7% rated it very important. For question 25, 45.8% stated it important to direct use of commercial products to institutionalize standardization and reduce duplication; 25% were neutral and 12.5% stated it somewhat important. For question 26, 70.8% rated it important to have policies which assign specific and detailed information security

management responsibilities to organizational leaders; 12.6% rated it neutral to not important. For question 27, 52.2% believed the degree to which FISMA's policies ignore the constraints placed on smaller segments of society or organizations is average; 30.4% state it is high to extremely high.

For question 28, 45.8% stated it somewhat important to neutral to enact information security controls incrementally so the cultural change impacts would not be dramatic; 16.7% rated it not important and 37.5% rated it important to very important. For question 29, 41.7% believed it important to classify information so it can be protected during information sharing and collaborative sessions; 16.6% rated it somewhat important to not important and 25% rated it very important. For question 30, 33.3% of the respondents believed the degree to which over classification of information hampers information sharing is average; 50% rated it high to extremely high and 16.7% rated it low. For question 31, 45.8% of the respondents thought it important to use process, data, and technology standardization and simplification techniques, instead of fixed controls, to meet information security goals; 33.3% were neutral.

Federal Information Security Management Act (FISMA) Correlation Analysis

In table 5, themes 23 and 29 indicated a low, or average, affirmation whereas theme 25 reflects a strong positive affirmation for the literary research position. The remaining themes show a moderate to strong positive response as a larger percentage of the responses supported the statements.

Table 5

Governance principles

Nbr	Theme Descriptions Federal Information Security Management Act Principles	Survey Ratings
22	Avoid over quantification of control measures to make them better.	65.2% - Average degree
23	Federal Information Security Management Act (FISMA) of 2002 has standardized the methodology used to provide a consistently repeatable information assurance program for use throughout the federal government.	50% - Important
24	Provides minimum set of controls specified in policy publication. Improves management oversight by directing appointment of key leaders like the chief information officer.	45.8% - Important
25	Dictates use of commercial products to institute standardization and reduce duplicative expenses.	70.8% - Important
26	Directly assigns specific and detailed responsibilities to individual government agency leaders.	52.2% - Average
27	Avoid a one size fits all implementation approach that ignores the constraints placed on smaller segments of an organization or society.	29.2% - Important
28	Implement controls incrementally so cultural change impacts are not so dramatic.	40.7% - Important
29	Ensure information sharing and collaboration are not hampered by over protection (classification) of information.	33.3% Average
30	Pay attention to process, data, and technology standardization and simplification techniques that can be as effective in achieving organizational goals as controls.	45.8% - Important

Survey Results Assessment

Figures 11 – 15 identify the survey results of the various themes that were developed from the literary research material. There appears to be general agreement with the research statements in most cases: quantification of control measures, dictating use of commercial products, over classification, and classification of information responses.

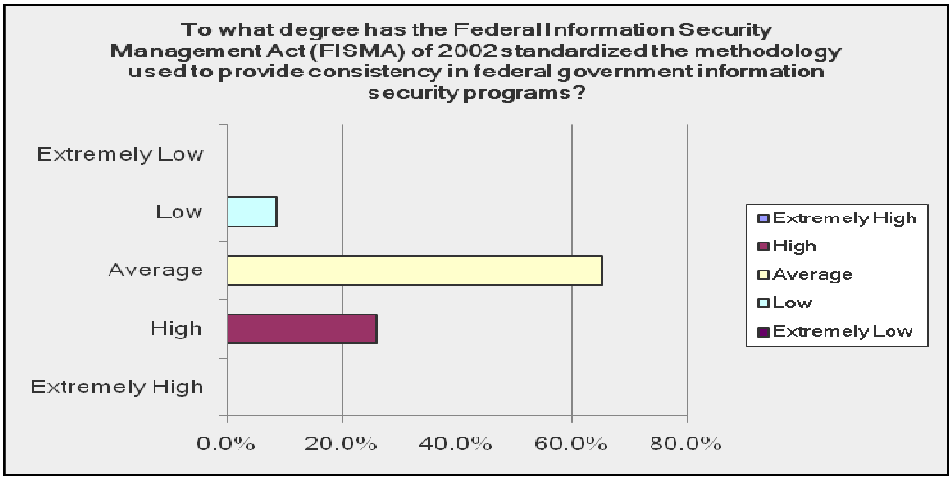

Figure 11. FISMA standardization of methodology

Average level of agreement in avoiding over quantification of control measures to make them better.

Figure 12. Use of commercial products

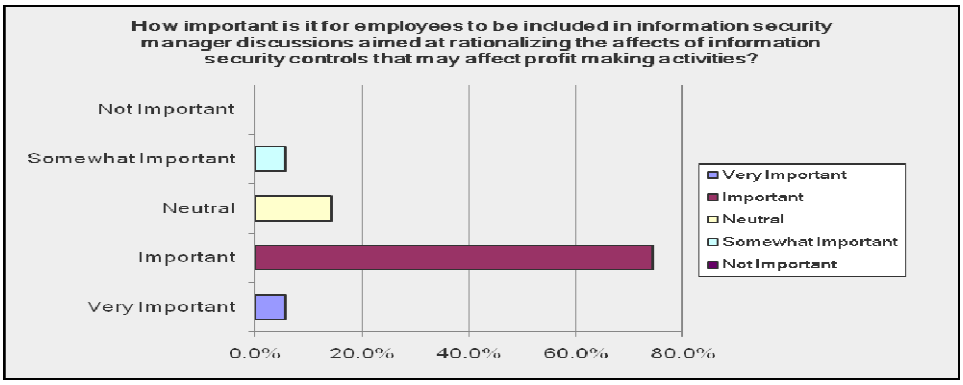

Figure 13. Dictate use of commercial products

High level of affirmation to dictates use of commercial products and to institute standardization and reduce duplicative expenses.

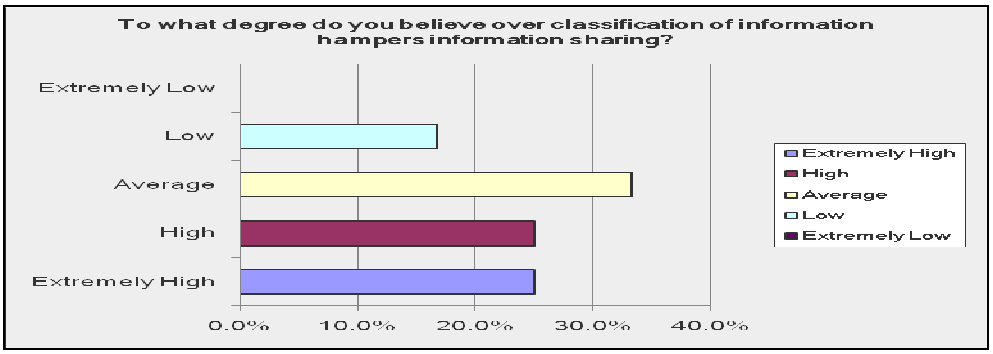

Figure 14. Over classification of information

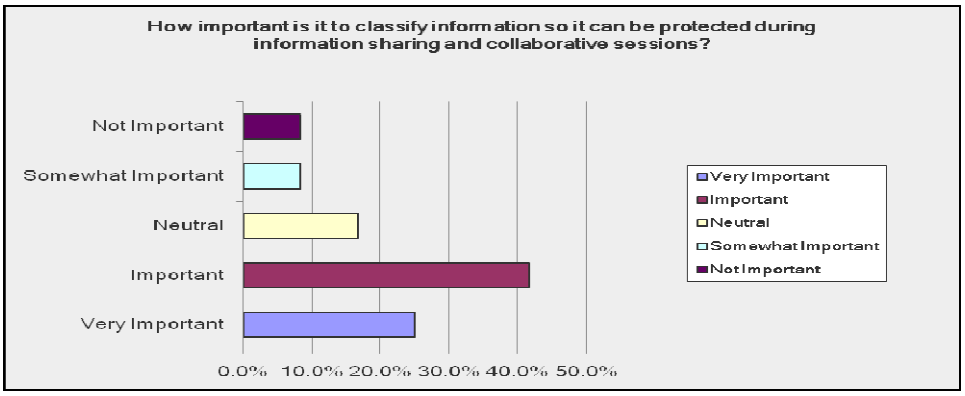

Figure 15. Classification of information

Low degree of affirmation to ensure information sharing and collaboration are not hampered by over classification of information. There appears to be a high level of agreement it is important to use a classification system to protect information.

Governance Principles

This section's narrative and table 6 summarize the responses received from questions 32 – 41 on the survey questionnaire at Appendix A.

Table 6

Governance response

Question	Percent	Response (Important – Very Important)
32	54.5%	Important to have a governance framework
33	31.8%	Neutral on the degree of government transparency/power sharing
34	38.1%	Neutral on the importance of regulating open/closed networks
35	40.9%	Neutral on role of government as a mediator/enforcer
36	38.1%	Low belief that less powerful entities are under represented
37	50.%	Governance policies lead to better security outcomes
38	45.5%	Remain open to new technologies and innovations
39	36.4%	Important policies are seen as creating favorable conditions
40	45.5%	Individual must be able to trust e-governance principles
41	31.8%	Average to high degree of non transparency and unfairness

For question 32, 54.5% of the respondents indicated it important to have a governance framework that balances the need for information technology and governance

rules; 31.8% rated it very important and 13.6% somewhat important to neutral. For question 33, 31.8% of the respondents stated the degree they felt there was a lack of balance and transparency in government power sharing with the IT community, business sector, and non profit organizations was average; 27.3% rated it low and 40.7% rated it high to extremely high. For question 34, 38.1% were neutral on deciding how important it is to regulate open and closed network systems, through governance, to address economic and geopolitical issues; 23.8% rated it important and another 23.8% rated it very important.

For question 35, 40.9% were neutral on assessing the importance for the government to serve as a mediator or enforcer in debates or discussions about information systems security governance and regulation; 13.6% rated it somewhat important and 4.5% rated it not important; a total of 40.9% rated it from important to very important. For question 36, 38.1% rated the degree to which they believed governance processes are weakened because of less powerful entities or minority groups are under represented is low; 28.6% rated it high and 9.5% extremely low. For question 37, 50% thought it important to have a strong correlation associated with better IT security outcomes and implemented governance policies. For question 38, 45.5% stated it important for organizations to remain open to new techniques or methods of governance.

For question 39, 36.4% stated the degree to which it is important for governing policies to be seen as creating favorable conditions for private enterprises and placing responsibility with citizens and employees was average to high. For question 40, 45.5% stated it is important for individuals to have trust in electronic governance policies,

methods, and procedures. For question 41, 31.8% believed weak public sector management, lack of policy making transparency, perceived unfairness in the rule of law, and a lack of openness was average to high.

Governance Principles Correlation Analysis

At table 7, themes 32, 33, and 35 indicate a low affirmation of the position stated in the literary research. The remaining themes show a strong positive response as a larger percentage of the responses supported the research statements.

Table 7

Governance principles

Nbr	Theme Descriptions	Survey Ratings
31	Establish a governance framework that is responsive to regulatory guidelines, treats information technology as both a governance and technology issue.	54.5% - Important
32	Lack of balance and transparency in government power sharing with experts in the IT community, business sector and non profit organizations.	31.8% - Average
33	Open and closed network systems are not sufficiently regulated, through governance, to address new economic and geopolitical issues.	38.1% - Neutral
34	Government is not taking the position as a mediator or enforcer to ensure a debate forum is established.	40.9% - Neutral
35	Legitimization of governance processes is weakened because smaller sectors of society (e.g. non profits) are under represented in collaborative discussion forums.	38.1% - Low degree
36	The positive correlation between strong governance and better IT outcomes/results is under estimated.	50% - Important
37	Organizations are not open to new techniques of governance: new arrangements, organizational patterns, and forms of knowledge production.	45.5% - Important
38	Governing policies are not seen as creating favorable conditions for private enterprises and placing responsibility with citizens/employees to emphasize individualism and entrepreneurialism.	36.4% - Average to High degree
39	Lack of trust people place in electronic government is still very low.	45.5% - Important
40	Weak public sector management with accountable institutions, lack of policy-making transparency, perceived unfairness in the rule of law, and lack of openness to citizen/employee participation detract from the effectiveness of governance policies.	31.8% - Average to High degree

Survey Results Assessment

Figures 16 – 18 identify survey result assessments of the various themes that were developed from the literary research material. There appears to be general agreement with the research statements in most cases: balance and transparency, regulation and governance, and government mediation responses.

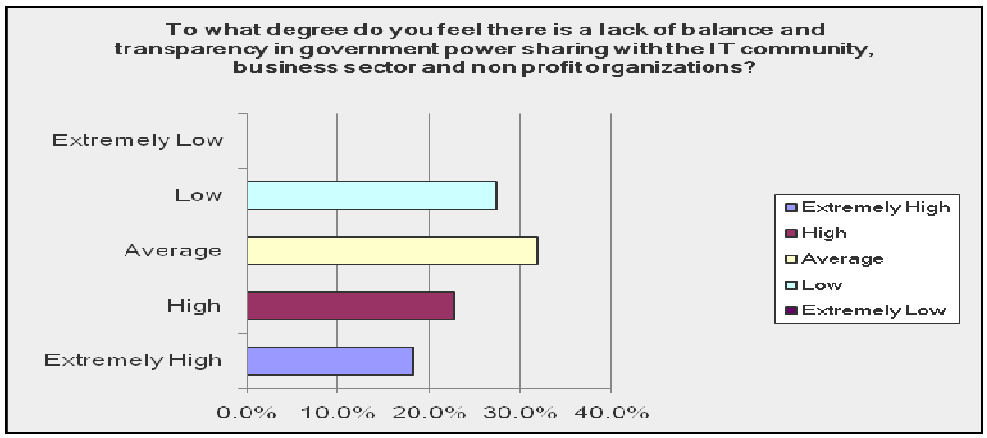

Figure 16. Lack of balance and transparency

Low level of affirmation (average) that there is a lack of balance and transparency in government power sharing with experts in the IT community, business sector and non profit organizations.

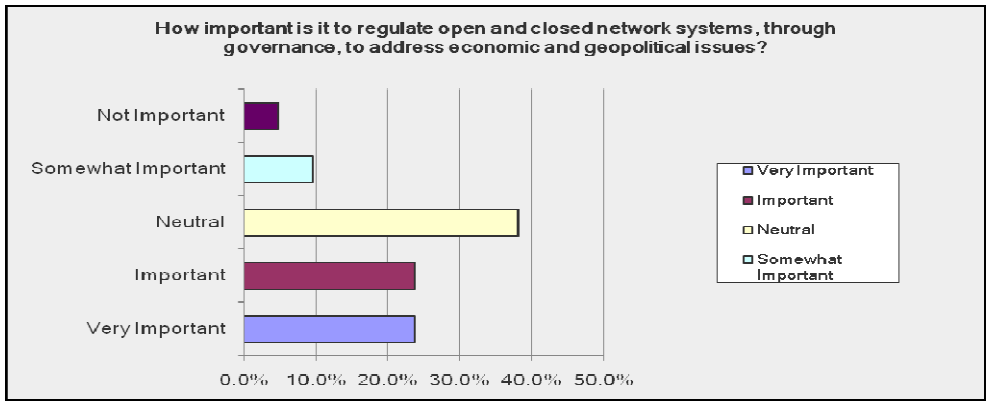

Figure 17. Favor regulation via governance

Low level of support that open and closed network systems are not sufficiently regulated through governance to address new economic and geopolitical issues was rated neutral.

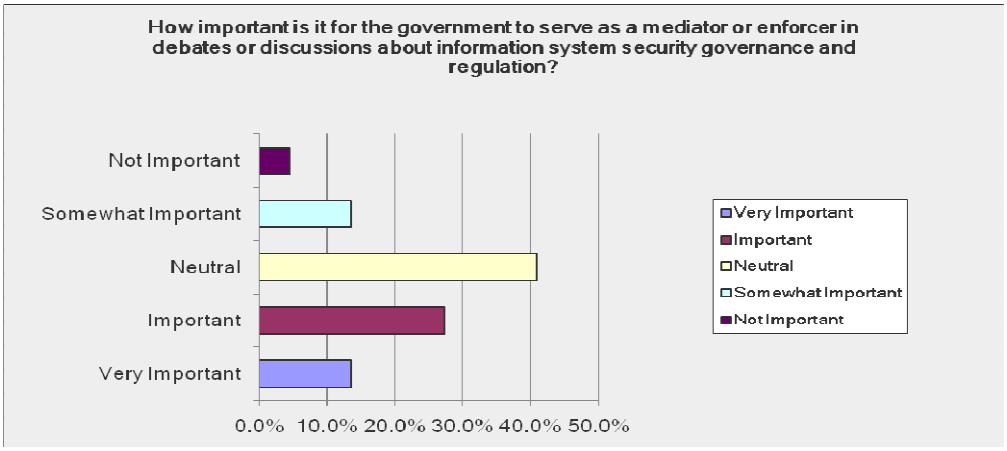

Figure 18. Favor government mediation

Low level of agreement that the government is not taking the position as a mediator or enforcer to ensure a debate forum is established was rated neutral.

Conclusions

Some of the barriers to establishment, potential benefits, prevalence, and critical success factors associated with security management and governance from the perspective of federal government management professionals in the field were identified and described in this chapter. The results of the analyses that were conducted to address the major research questions of the research study were presented in this chapter. The initial section of the chapter presented the results of the pilot study that was undertaken before the main data collection procedures started. Descriptive statistics were presented for the sample of security professionals who participated in the present study. The main body of the chapter addressed each of the three research questions posed in the basic research framework. The three basic research questions were listed with the associated

themes or survey question assessments. Correlation and analysis of the survey responses to each question was performed to determine the positive, neutral, or negative nature of the responses. Specifically, any positive affirmation, deviations or surprising responses were analyzed and assessed.

Question 1: How can management practices be improved in the federal government sector of society to respond to current and emerging information technology security issues? Correlation and analysis of the information system security management and governance survey results revealed the following general results. The figure 19 questions 1, 2, 14, 15, 20, and 21 have a strong positive affirmation of the positions developed from the literary research. Question 3 respondents indicated a low affirmation for the literary research position. The remaining questions indicate a positive affirmation because a larger percentage of the responses supported the statement. Assessment of specific deviations indicated general agreement with the research statements in most cases. Deviations are noted in the areas of assessing individual user behavior, observing and analyzing behavioral changes, impact of staff and line changes on implementing security controls, managing the increase in information, addressing people, process, technology concerns in policies, innovation social impacts, and rationalizing the affects of controls on society.

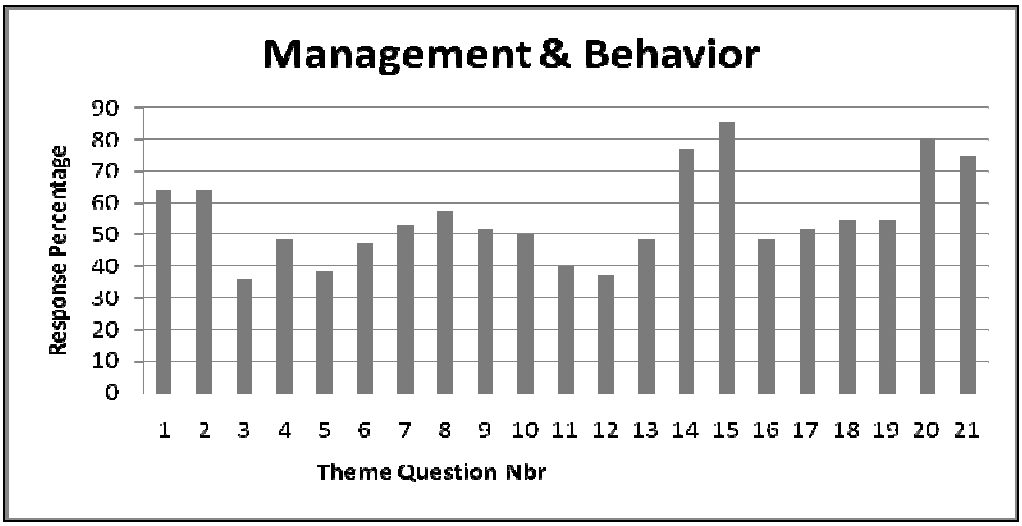

Figure 19. Management & behavior

Question 2: How has the federal information security management act contributed to improving IT security governance and management in the federal government? Correlation and analysis of the second research question for federal information security management act (FISMA) principles revealed the following general results. Figure 20 shows that questions 22 and 25 indicated a high affirmation for the literary research position. The remaining themes show a moderate to strong positive response as a larger percentage of the responses supported the statements. Assessments of specific deviations in this area indicated general agreement with questions that were developed from literary research material. There appears to be general agreement with the research statements in most cases. The deviations are in the areas of quantification of control measures, dictating use of commercial products, over classification, and classification of information responses.

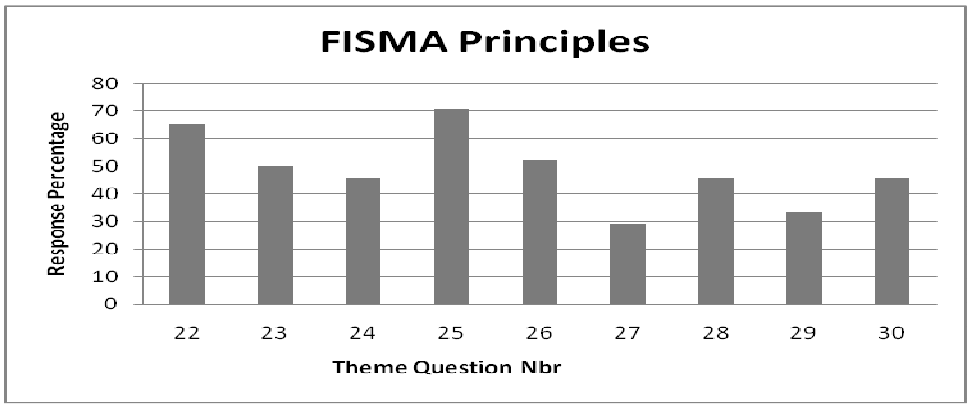

Figure 20. FISMA responses

Question 3: Why are IT security governance practices not more effective in responding to current and emerging IT security issues? Correlation and analysis of the third research question for governance principles revealed the following general results. Figure 21 shows that questions 32, 35, and 40 indicated a low affirmation of the position stated in the literary research. The remaining questions showed strong positive response and a larger percentage of the responses supported the research statements. Assessments of specific deviations in this area indicated general agreement with themes that were developed from literary research material. Deviations in the areas of balance and transparency, regulation and governance, and government mediation responses were noted.

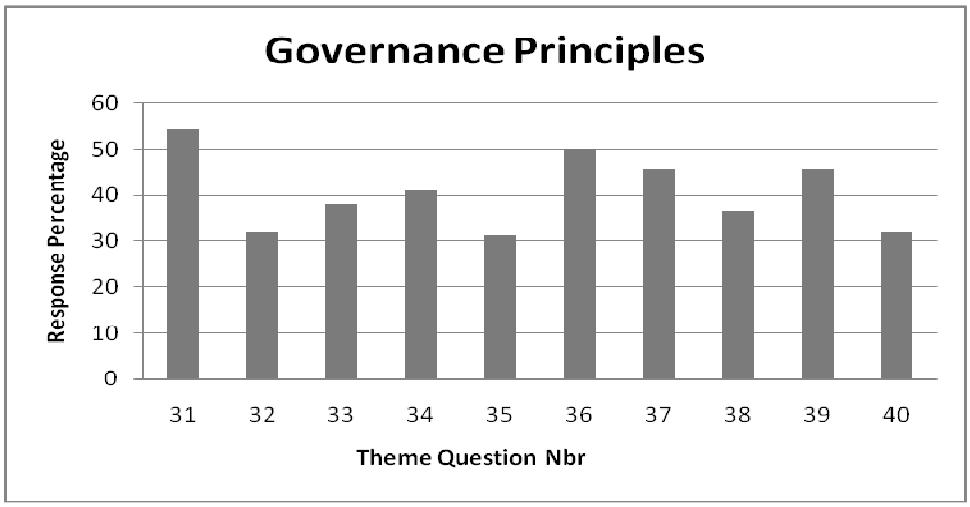

Figure 21. Governance responses

In chapter 5 the research problem is briefly explained, conclusions, social change implications, a summary, and recommendations for future research are also presented.

Chapter 5: Discussion, Conclusions, and Recommendations

Information systems security models and frameworks do not sufficiently emphasize the human element as a cause and solution to widespread security problems resulting from technical innovations. Instead, technological solutions are the primary means being pursued throughout the federal government to solve what is largely a management and behavioral issue (Kolb & Abdullah, 2009). The pacing factor for innovation should first be the lack of focus on managerial and behavioral issues and then the technological solutions (Kolkowska, 2004). Deloitte and Touche's (2007) research survey results supported the need for increased attention on the human factor as the root cause of information security failures. Training programs were developed, policies issued, and governance processes implemented to reduce security problems; however, Baker and Wallace (2007) identified people as the weakest link in implementing viable security policies. Despite this research finding, the latest GAO (2009) report suggested implementing technical controls as the best solution to manage security risk throughout the government.

Chung (2007) also challenged the notion that security controls are the best solution to address security challenges. Chung uncovered the paradigm shift that has introduced new social norms, ethical values, and cultural trends that are impervious to technical control mechanisms alone. In a broader context, Lobree (2002) and Volonino, Gessner, and Kermis (2004) showed how legislation was enacted in response to corruptness, and industry cries for rules, regulations and standardization to regulate government and electronic commerce. Landell-Mills (2003) expressed the importance of

implementing multidisciplinary leadership and management approaches to balance the policies and governance structures. I sought explanations for why current governance practices have not been more effective, conducted extensive literary research, and synthesized information to reveal prominent challenges. The social impacts identified in the literature research revealed central research opinions and recommendations that supported the need for improved behavioral management and governance to address information security challenges.

The theoretical and conceptual framework used to conduct this research were McGregor's (1960) theory X and theory Y principles integrated with the theories espoused by Weber (1962) and Fayol (1987). Theory X posits indicate that employees are inherently lazy so they must be closely monitored and supervised. Theory Y posits indicate employees are self motivated so less control and supervision is required. The study was conducted by explicating the problem through the proposed research questions and conducting deductive analysis to revel seminal themes, ideas, and opinions.

The research was designed as a qualitative analysis methodology because the intent was largely discovery. A survey questionnaire was used as the research instrument to collect the ideas and opinions of federal government employees as a basis to assess which research themes were deemed most relevant in resolving information security problems. These seminal themes were seen as Drucker's (2008) proper fit region between managerial behavior, federal security management policies, and governance principles. The literature review process helped further refine the research questions and established the theoretical and practical relevance necessary to help shape the study methodology.

Summary Research Analysis

Following the guidance expressed by Leedy and Ormrod (2005), the three research questions were designed as triangulation points from which the problem could be explored. Responses to question 1: Management practices in the federal government sector of society can be improved to respond to current and emerging information technology (IT) security issues by:

1. Assessing employee behavior after implementing security controls
2. Observing and analyzing behavioral changes (cause and effect)
3. Establishing differing levels of controls
4. Developing legal constructs that follow existing laws
5. Tying innovation initiatives to business strategy/mission
6. Factoring in anticipated social impacts early
7. Including employees in policy development discussions

The responses represent the seminal themes that managers can use to help develop their information systems security policies and guidelines in the federal government. The management and behavioral practices uncovered by past and present theorists are still relevant. It is feasible that the theory X and Y model can be used to find a proper fit between the interests of the business, employee, and security protection.

As policies, either technical or procedural, are implemented it is essential to look at the second and third order behavioral effects that result from putting security controls in place. The proliferation of information and innovations are not going to stop so

managers must accept this eventuality and structure their organization and management strategies accordingly. Decision making processes should include a synthesis of available information and be moderated by behavioral, cultural, and social influences.

Three key elements of the decision making process that must be addressed are people, processes, and technology. Addressing these elements individually and then in an integrated manner can help find the solutions that are the proper fit for specific businesses and situations. Whenever new business ventures or policies are being considered it is important to analyze and focus on the impending social impact early in the decision making process. In certain situations, the technical solution will not fit within the culture or causes such a major social change that it is not implementable until internal and external environmental factors are modified. Non automated changes in processes may be the preferred solution because of social impacts.

Profits, or mission success in the federal government, are often the driving factor for business decisions so it is important to be engaged in discussions about regulating changes to institute information security management controls. New innovative solutions that pose more risk to business's security posture can require regulation to force fixes for the security vulnerabilities before they are allowed to enter the market place. The federal government has been a leader in this area in the past and should continue helping balance the innovative nature of businesses with the need for security protections.

Response to question 2: The FISMA can contribute to improving IT security governance and management in the federal government by:

1. Avoiding over quantification of control measures to assess effectiveness

2. Using commercial products for standardization benefits
3. Avoiding over classification to protect information – inhibits sharing

In terms of over quantification of control measures, the larger percentage of responses did not see a problem with over quantification of control measures affecting the effectiveness of FISMA. Literary research indicated there was a strong tendency in the federal government to over quantify the effects of controls using metrics. FISMA's contributions to improving information security management in the federal government was not supported with a large percentage of the survey responses; approximately half believed its contributions were important in bringing about standardization and consistency.

The use of commercial products as a method of forcing standardization was supported by the literary research and survey responses. There is a strong belief that commercial products offer standardization and interoperability. Literary research provided a strong argument that the government had a tendency to over classify information and this inhibits broader information sharing (Conner et al., 2003). The research suggested the need to moderate this tendency through policies; however, the federal government survey respondents in my research did not to agree that over classification was a major problem.

Responses to question 3: IT security governance practices can be more effective in responding to current and emerging IT security issues by:

1. Creating balance and transparency between business and government
2. Regulating open and closed network systems through governance

3. Mediating and enforcing in debates and discussions

The need for a governance framework that is synchronized with regulatory guidance was noted as important. Also, the balance between governance and technology innovation was underscored. The federal government employees seemed to agree that strong governance leads to successful IT implementations that do not stifle innovation or adversely affect business operations.

Implications for Social Change

The behavior of individuals, regardless of social settings, continues as the prime causes of information security problems. As more and more innovations are introduced into the market space managers must learn how to affect behavior that respects information security principles the same as people obey home security, school and traffic rules within the many cultures that comprise society. This research study identified four areas that have major implications for social change: Focusing on the individual's behavior should help better understand the triggers of change, staff and management relationships, knowledge worker motivations, and the affects of controls on people. This knowledge will help institute management and governance processes that foster a healthy social change environment where innovation can thrive.

The significance of this information security management research is that it seeks to integrate the theories of prominent human management researchers with literary research in information security management and governance. Central ideas or themes that were noted as challenges, suggestions, and general research observations were extracted from the research study. The synthesis of these research ideas can help guide

future research in this area and provide insight in developing future governance policies or legislation to enhance information security without undue restrictions to innovation. This research will also help focus attention on the human management aspects of ensuring governing information security controls are properly implemented and followed.

Managers still have not fully grasped the necessity to balance the technical and management controls to achieve optimum effectiveness at reasonable costs (Ionescu, 2009). Therefore, this study can help inform training and education programs so the risks can be reduced from attacks inside or outside the environment. These research themes can also help the Department of Commerce efforts toward implementing rigorous and detailed security control programs for the federal government. This study amplified areas where future research is needed to moderate government regulations on information system security controls. Subsequent laws in the privacy, data protection, and medical areas are further examples of the importance of government intervention to moderate social behaviors. Despite the success of the many technical solutions that have been developed as information security controls, the human dimension needs comparable research attention (Fraser, 2007). A synthesis of literary research and survey information that can be used as strategic guidance in developing governance rules to protect broader organizational or societal interest is developed from this research.

Recommendations for Action

In order to find the most effective solution to a problem it is helpful to look at it from several different perspectives. McGregor's (1960) theory X and Y models provided a framework that can be used to establish management, behavior, and governance

principles that are effective in reducing information security problems. Further research should be undertaken to examine the behavioral implications associated with the implementation of IT security controls. Understanding these implications can lead to the development of more effective rules that recognize and balance the individual behavioral aspects of security control actions with reality.

Research could also be furthered by including individual behavioral criteria in investigation and inspections in federal GAO or inspector general programs. The GAO investigation reports are initiated under the authority of the office of management and budget or congress so research findings are linked to budget, policy, governance, and legal entities in the federal government. The government can better inform itself about directing IT security expenditures to gain maximum effect and benefit. The themes developed in this research study should also be used to further quantitative studies of the effects of implementing controls on individuals in government organizations. Is an organization more secure if it has very strict security control policies; compared to one with lesser restrictions?

Researcher Experience Reflection

Hancock and Algozzine (2006) asserted that although the type and scope of questions are without limits they all share a common characteristic of a desire to find the answer to a question. Reflecting on this research process, it was essential to develop and frame research questions before starting literary research. Although the questions were developed first, the research material led to further refinement and restatement of the questions. It was not the pure inquisitiveness of the researcher that shaped the questions

but the body of research material as well. Building a research road map was an important element of the idea or question development process. What was to be studied, how to study (design), who to study, how to gather information, how best to analyze the information, who to share findings with, and how to confirm findings were the essential elements of the plan used to guide research studies.

Understanding the important distinctions between inferential and descriptive research ensured the proper approach is undertaken. The desire to generalize beyond a specific group about a larger population must be approached as inferential research, whereas, collecting information to describe the group at hand follows descriptive research guidelines. Although initial analysis of the research study indicated a quantitative analysis methodology would be feasible, research material and the framing of the research questions led to qualitative analysis. In order to ground the research in theory, management and behavioral research theories were the most revealing. The most difficult part of research for this project was determining what theoretical lens was appropriate and beneficial in descriptive research. A triangulation of behavioral management, government policy, and governance were selected after looking holistically at the results of the exhaustive research study.

As a 26 year military officer in the information technology profession it was important to ensure those personal views and biases did not enter into the research. Living through the era of constant information technology change in the military and attempts to establish controlling policies shaped my initial thinking about answers to the research questions. Literary research validated many of the thoughts but did not support

others. Initial indications were that strong governance would lead to improvements in an organization's overall security posture. The research study results supported the need for strong governance but focused heavily on a weakness of being able to govern the individual. The weakest link, largest problem, and common mistakes seemed to be directed back to an individual who, for whatever reasons, did not follow the rules. The focus of the federal government was heavily weighted toward finding automated solutions to resolve access control security problems that the individual caused for a multitude of unknown reasons.

My research preconception was that other researchers had not recognized and studied the behavior of individuals as prime causes for information security problems. After extensive research it was easy to see there were qualitative research studies calling for more attention in this area. It was surprising that some brave researchers had completed quantitative research studies that were based on the systems theory to offer decision-making frameworks and analysis models. This research study has enlightened my thinking about information security and changed my view about how best to address the core of the issue. It is more about the individuals, just as it was in the beginning theories about behavior and management. The innovative tools still have value; however, without the employee's buy in the organization has a very pervasive information security vulnerability that will impact its goals and mission accomplishment.

Conclusions

The goal of the research study was to foster social change through discovery and analysis of ways to address information security problems in the federal government, increase understanding of key issues so the root cause of security vulnerabilities can be remediated, and find management and governance principles to continue shaping the information security landscape to embrace innovation while reducing risks posed by employees. The study was rooted in basic management and behavioral theories and extracted central ideas or themes from exhaustive literary research. The themes were synthesized into key recommendations that federal government managers can use to address security problems.

Social change will be realized in training and education program improvements, implementing rigorous security control programs in the federal government, amplifying areas where future research is needed to moderate government regulations, and inform discussions about establishing laws aimed at moderating social behaviors. Key issues were uncovered from research and validated by survey of government employees to understand the root causes and proposed remediation for security problems. The individual employee was identified as the root problem and several ideas developed to help managers address this largely behavioral issue with technology, governance, and management approaches.

Several key and essential management and governance principles, the proper fit, were developed to help continue shaping the information security landscape and reduce impacts on innovation initiatives.

1. Assess employee behavior after implementing security controls
2. Observe and analyze behavioral changes (cause and effect)
3. Establish differing levels of controls
4. Develop legal constructs that follow existing laws
5. Tie innovation initiatives to business strategy/mission
6. Factor in anticipated social impacts early
7. Include employees in policy development discussions
8. Avoid over quantification of control measures to assess effectiveness
9. Use commercial products for standardization benefits
10. Avoid over classification to protect information – inhibits sharing
11. Create balance and transparency between business and government
12. Regulate open and closed network systems through governance
13. Government must mediate and enforce in debates and discussions

McGregor's (1960) X and Y theories were used as the lens to discuss implementing the best set of management controls that will properly influence employee's behavior. The theory called for a model to balance controls needed to motivate the unmotivated and self motivated employee.

This proper fit is represented by the 13 governance and management principles in the Venn Diagram at Figure 22. As principles like these are highlighted as essential management elements in information systems security policies and governance, social changes will encounter less friction so innovation can thrive without adversely impacting the balance required in a diverse society.

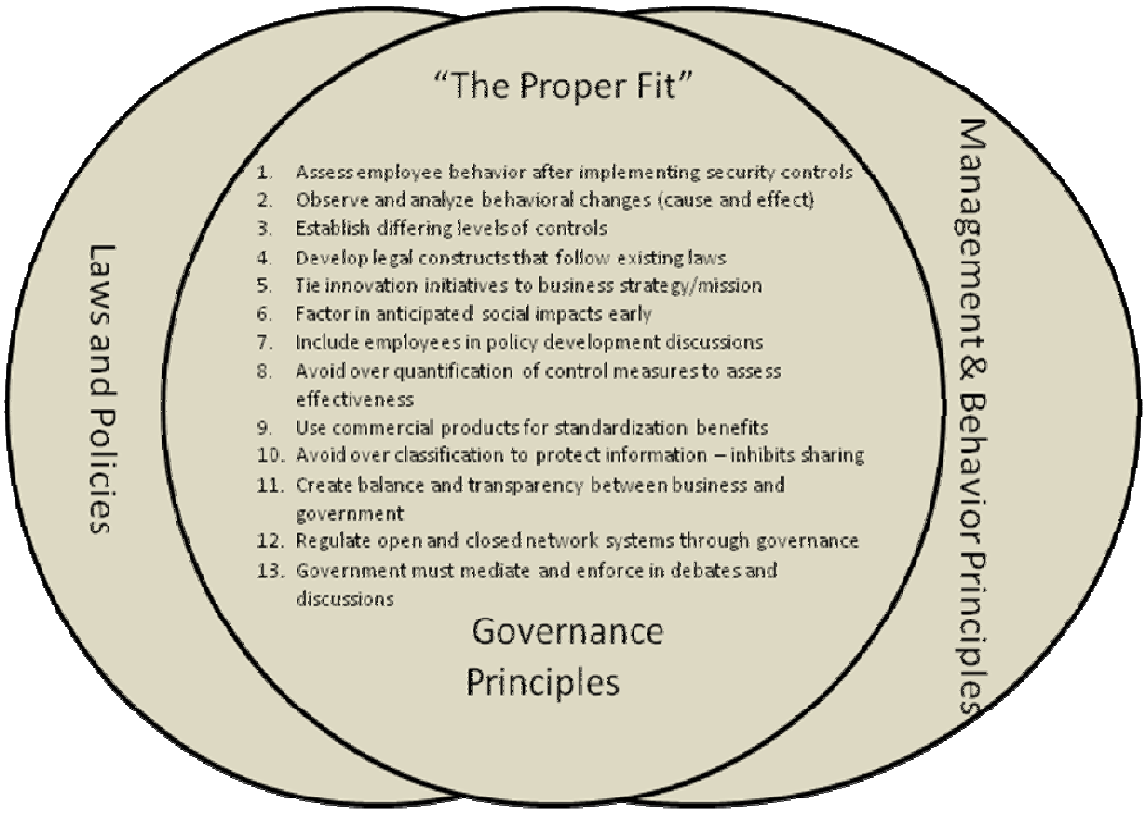

Figure 22. The proper fit

References

Aczel, A. & Sounderpandian, J. (2009). *Complete business statistics.* New York: McGraw-Hill Irwin.

Alfaro, J., Boulahia-Cuppens, N., & Cuppens, F. (2008). Complete analysis of configuration rules to guarantee reliable network security policies. *International Journal of Information Security*, *7*(2), 103-122.

Baird, Z. (2002). Governing the Internet. *Foreign Affairs*, *81*(6), 15-20. Retrieved from http://www.foreignaffairs.com/articles/58427/zoe-baird/governing-the-internet-engaging-government-business-and-nonprofi.

Baker, W., & Wallace, L. (2007). Information security controls: Is information security under control?. IEEE Security & Privacy, *IEEE Computer Society.* 36-44.

Brown, A., & Grant, G. (2005). Framing the frameworks: A review of IT governance research. *Communications of the Association for Information Systems. 15*, 696-712.

Chung, I. (2007). Roles and impacts of IT on new social norms, ethical values and legal frameworks in shaping a future digital society. National Science Foundation. Speakers position paper. 1-3. Retrieved February 10, 2011 from http://www.oecd.org/dataoecd/43/13/38818332.pdf.

Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, May 2003.

Conner, B., Noonan, T., & Holleyman, R. (2003). Information security governance: Toward a framework for action. *Business Software Alliance*. Retrieved February 10, 2011 from http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx.

Creswell, J. (2007). *Qualitative inquiry & research design*. Thousand Oaks, CA: Sage Publications, Inc.

De Haes, S., & Grembergen, W. (n.d.). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management.* (26), 123-137.

Deloitte & Touche. (2005). 2005 Global Security Survey. Retrieved February 10, 2011 from http://www.deloitte.com/view/en_MK/mk/industries/financialservices/42b88e6bc220e110VgnVCM100000ba42f00aRCRD.htm.

Deloitte & Touche. (2007). 2007 Global security survey: The shifting security paradigm. Retrieved February 10, 2011 from http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf.

Dodd, R. (2005). How does information security fit into a governance framework?. *Information Systems Journal*. 1-2. Retrieved February 10, 2011 from http://www.isaca.org.

Drucker, P. (2008). *Management: Revised edition*. New York: HarperCollins Publishers.

Edersheim, E. (2007). *The definitive Drucker.* New York: McGraw-Hill.

Ezingeard, J., Bowen-Schrire, M., & Birchall, D. (2004). Triggers of change in information security management. Retrieved February 10, 2011 from http://www.information-institute.org/security/3rdConf/Proceedings/.

Fayol, H. (1987*). General and industrial management.* Belmont, CA: David S. Lake Publishers.

Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C @ 2458 (2002).

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Fraser, N. (2007, April). Creating model citizens for the information age: Canadian internet policy as civilizing discourse. *Canadian Journal of Communication*, *32*(2), 201-218.

Goo, J. (2009). The role of service level agreements in relational management of information technology outsourcing: An empirical study. *MIS Quarterly*, 33(1), 119-145.

Government Accountability Office (GAO). (2009). Cybersecurity: Continued efforts are needed to protect information systems from evolving threats. GAO-10-230T.

Grubb, T., & Burke, T., (2008). A framework for governance, risk management and compliance. Retrieved February 10, 2011 from http://www.graberassociates.net/new/documents/Grubb-Burke_BAF_21-03_08.pdf.

Hancock, D., Algozzine, B. (2006). *Doing case study research.* New York: Teachers College Press.

Herath, T., Herath, H., & Bremser, W. (2010). Balanced scorecard implementation of security strategies: A framework for IT security performance management. *Information Systems Management*, *27*(1), 72-81.

Hersey, P., Blanchard, K., & Johnson, D. (1996). *Management of organizational behavior: Utilizing human resources.* Upper Saddle River, NJ: Prentice Hall.

Hoover, J. (2009a). Techstrategy: Cybersecurity balancing act. *InformationWeek,*1228. 46.

Hoover, J. (2009b). White House turns up heat on agencies. *Information Week*, 1239. 16.

ICANN. (2009). Home. Retrieved February 10, 2011 from http://www.icann.org/en/about/.

Industrial College of the Armed Forces. (n.d.). ICAF mission. Retrieved February 10, 2011 from http://www.ndu.edu/icaf/mission/index.htm.

Ionescu, L. (2009). Organizational values, managerial leadership, and personal effectiveness. *Annals of Spiru Haret University, Journalism Studies*, *10.*126-130.

Kolb, N., & Abdullah, F. (2009). Developing an Information Security Awareness Program for a Non-Profit Organization. *International Management Review, 5*(2), 103-107.

Kolkowska, E. (2004). Managing of information security with consideration of individual values and organizational form. PHD project. Orebro University, Sweden, 1-15, Retrieved February 10, 2011 from, http://www.information-institute.org/security/3rdConf/Proceedings/23.pdf.

Korotka, M. (2004). Information assurance technical framework: An end user perspective. Retrieved February 10, 2011 from, http://www.information-institute.org/security/3rdConf/Proceedings/.

Ladan, S., Yari, A., & Khodabandeh, H. (2006, May). Combination of information security standards to cover national requirements. *Enformatika*, *13*, 148-152.

Lamour, J. (2008). Impact of User Awareness and Training of InfoSec Practitioners on Data Security (Doctoral Dissertation, Applied Management and Decision Sciences, Information Systems Management, College of Management and Technology Walden University). (UMI No. 3291620). Minneapolis, MN.

Landell-Mills, P. (2003). Coming to grips with governance: the lessons of experience. *Journal of Contemporary China*. Retrieved February 10, 2011 from http://www.informaworld.com/smpp/content~content=a713675898~db=all~order=page.

Leedy, P., & Ormrod, J. (2005). *Practical research: Planning and design.* Upper Saddle River, NJ: Prentice Hall.

Le Grand, C. (2003). Audit & Security Controls That Work: Information Security Governance and Assurance. *Institute of Internal Auditors*. Retrieved February 10, 2011 from http://www.theiia.org.

Lobree, B. (2002, November). Impact of legislation on information security management. *Information Systems Security*, *11*(5), 41-48.

Luo, X. & Warkentin, M. (2004). Assessment of information security spending and costs of failure. Retrieved February 10, 2011 from http://www.information-institute.org/security/3rdConf/Proceedings/.

Malcolm, J. (2008). Appraising the success of the internet governance forum. *IT Governance Institute*. Retrieved February 15, 2011 from http://www.internetgovernance.org.

Mathiasen, N. (2008). Investigating how everyday people experience security. Symposium On Usable Privacy and Security (SOUPS) 2008, July 23-25, 2008, Pittsburgh, PA. Retrieved February 10, 2011 from http://cups.cs.cmu.edu/soups/2008/posters/mathiasen.pdf.

Masurkar, V. (2004). On developing a methodology for managing security vulnerabilities. Retrieved February 10, 2011 from http://www.information-institute.org/security/3rdConf/Proceedings/.

McFadzean, E., Ezingeard, J. & Birchall, D. (2004). Anchoring information security governance research: Sociological groundings and future directions. Retrieved February 10, 2011 from http://www.information-institute.org/security/3rdConf/Proceedings/.

McGhee, W. (2008). *Information Technology Governance: An Exploratory Study of the Impact of Organizational Information Technology Security Planning (Doctoral Dissertation, School of Business and Technology Capella University).* (UMI No. 3296824), Minneapolis, MN.

McGregor, D. (1960). *Human side of enterprise*. New York: McGraw-Hill.

Mintzberg, H.(1989). *Mintzberg on management: Inside our strange world of organizations*. New York: The Free Press.

Mitrakas, A. (2006). Information security and law in Europe: Risks checked?. *Information and Communications Technology Law,* 15(1). 33-53.

Mueller, M., & Chango, M. (2008). Disrupting global governance: The Internet Whois service, ICANN, and privacy. *Journal of Information Technology & Politics*, 5(3), 303-325.

Myler, E., & Broadbent, G. (2006, November). ISO 17799: Standard for security. *Information Management Journal*, *40*(6), 43-52.

National Institute of Standards and Technology (NIST) Special Publication IR 7298, *Glossary of Key Information Security Terms,* April, 2006.

Nnolim, A. (2007). *A Framework and Methodology for Information Security Management (Doctoral Dissertation, College of Management Lawrence Technological University). (UMI No. 3296872).* Southfield, MI.

Nowell, C. (2007, September). Regulatory compliance - the wonderful world of FISMA. *Information Systems Security*, *16*(5), 278-280.

Nyanchama, M. (2005, July). Enterprise vulnerability management and its role in information security management. *Information Systems Security*, *14*(3), 29-56.

Oscarson, P. (2004). A scandinavian information systems perspective on security. Retrieved February 10, 2011 from http://www.information-institute.org/security/3rdConf/Proceedings/.

Pricewaterhouse Coopers. (2009). An Executive View of IT Governance. *IT Governance Institute*. Retrieved February 10, 2011 from http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=47365.

Saint-Germain, R. (2005, July). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60-66.

SANS Institute. (2006). The ten most important security trends of the coming year. Retrieved February 10, 2011 from http://www.sans.org/top20/2006/.

Sayer, A. (2006). *Methods in social science: A realist approach.* New York: Routledge.

Shah, M., Mohammad, M., Zaighman, M. & Azia, R. (2009). Organisational barriers in offering E-banking. *Journal of Electronic Commerce in Organizations.* 7(2). 67-82.

Siber Systems. (2007). Password management survey: IT managers respond to the impact of password policies on security and productivity. Retrieved February 10, 2011from http://www.isoftland.com/docs/roboform/info/RoboForm_Enterprise__Encuesta.pdfl.

Simonsson, M., Johnson, P., & Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. *Information Systems Management*, 27, 10-24.

Singleton, R. & Straits, B. (2005). *Approaches to social research.* New York: Oxford University Press.

Solomon, M., & Chapple, M. (2005). *Information security illuminated*. MA: Jones and Bartlett.

Stanton, J., Caldera, C., Isaac, A., Stam, K., & Marcinkowski, S. (n.d.). Behavioral information security: Defining the criterion space. School of Information Studies, Syracuse University, Syracuse, NY. 1-27.

Sweeney, A. (2007). Electronic Government-Citizen Relationships: Exploring Citizen Perspectives. *Journal of Information Technology & Politics,* 4(2). 101-116.

Sys, S. (2007). One Man's Anarchy. *Index on Censorship*, *36*(4), 86-87.

Tedre, M., Sutinen, E., Kähkönen, E., & Kommers, P. (2006, January). Ethnocomputering: ICT in cultural and social context. *Communications of the ACM*, *49*(1), 126-130. 10.

U. S. Department of Commerce. (2006a). Federal information processing standards publication: Minimum security requirements for federal information and information systems (National Institute of Standards and Technology (NIST), FIPS Publication 200). Gaithersburg, MD: NIST Computer Security Division.

U.S. Department of Commerce. (2006b, December). Recommended security controls for federal information systems. (National Institute of Standards and Technology (NIST), NIST Special Publication 800-53, Revision 1, Gaithersburg, MD: NIST Computer Security Division.

Volonino, L., Gessner, G., & Kermis, G. (2004, August). Sarbanes-Oxley links IT to corporate compliance. Proceedings of the tenth americas conference on information systems, New York, NY, 1-8.

Walsh, J., & Maloney, N. (2007). Collaboration Structure, Communication Media, and Problems in Scientific Work Teams. *Journal of Computer-Mediated Communication*, *12*(2), 378-398.

Weber, M. (1962). *Basic concepts in sociology*. Westport, CT: Greenwood Press Publishers.

Wijesinghe, H. & Karamat, P. (2004). A new model for the E-commerce security. Retrieved February 10, 2011 from http://www.information-institute.org/security/3rdConf/Proceedings/.

Wilshusen, G. (2008). U.S. Government accountability office testimony before the subcommittee on federal financial management government information. GAO-08-57IT.

Wittmann, A. (2009). Government IT: Ready for change-maybe. *Information Week.* 1243, 30.

Wu, Y. (2007). *Effects of IT Governance on Information Security (Doctoral Dissertation, Department of Management Information Systems in the College of Business Administration University of Central Florida).* (UMI No. 3377838). Orlando, FL.

Yin, R. (2009). *Case study research design and methods.* Thousand Oaks, CA: Sage Inc.

Appendix A: Research Consent Form

You are invited to take part in a research study of what information systems security governance and management principles are needed to support vice restrict innovation. You were chosen for the study because you are a senior management professional in the federal government. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher who is a doctoral student at Walden University.

Background Information:
The purpose of this study is to validate management and governance principles that will help managers design information security policies that are accepting of new technologies but do not inhibit employee productivity.

Procedures:
If you agree to be in this study, you will be asked to:

- Read this consent form – keep a copy for your records (10 minutes)
- Log on to a computer that has browser access to the Internet and click on the link provided in the e-mail (5 minutes)
- Read and select a response for each of the 41 research questions (30 minutes)
- Save your questionnaire and close the browser (30 seconds)

Voluntary Nature of the Study:
Your participation in this study is voluntary. This means that everyone will respect your decision of whether or not you want to be in the study. No one at ICAF will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind during the study. If you feel stressed during the study you may stop at any time. You may skip any questions that you feel are too personal.

Risks and Benefits of Being in the Study:
The normal risks associated with accessing the Internet are present so it is prudent to have virus protection software loaded and protect login and password information. As a federal government manager you may find the questions helpful in developing and executing policies in your department.

Compensation:
There is no compensation for being in this study.

Confidentiality:
Any information you provide will be kept anonymous. The researcher will not use your information for any purposes outside of this research project. Also, the researcher will not include your name or anything else that could identify you in any reports of the study.

Contacts and Questions:
If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 1-800-925-3368, extension 1210. Walden University's approval number for this study is 06-17-10-0385603 and it expires on June 16, 2011.

Appendix B: Survey Questionnaire

Information Systems Management and Governance

1. Are you an adult (above 17 years old)?

***MUST ANSWER**

- ☐ ☐ 1. YES
- ☐ ☐ 2. NO

This section is designed to focus on your thoughts about what specific management changes are most important to improve the information security posture in an organization.

2. How important is it to assess an employee's behavior after security controls are put in place?

- ☐ ☐ Very Important
- ☐ ☐ Important
- ☐ ☐ Neutral
- ☐ ☐ Somewhat Important
- ☐ ☐ Not Important

3. How important is it to observe and analyze behavioral changes to understand how the changes affect user's behavior?

- ☐ ☐ Very Important
- ☐ ☐ Important
- ☐ ☐ Neutral
- ☐ ☐ Somewhat Important
- ☐ ☐ Not Important

4. To what degree are changes in staff and line management relationships affecting a manager's ability to implement security controls (e.g. staff wants to be included in decision making process vice just receiving direction)?

- ☐ ☐ Extremely High
- ☐ ☐ Moderate
- ☐ ☐ Average
- ☐ ☐ Low
- ☐ ☐ Extremely Low

5. How important is it to have different levels or degrees of controls to secure information sharing sessions?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

6. How important is it to develop legal constructs for managers to ensure information security laws are understood and followed?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

7. How important is it to have command and control constructs in place to direct managers to comply with information security laws and/or policies?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

8. To what degree is it important to balance control, authority and motivation in persuading employees to follow information security guidelines?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

9. In today's information savvy culture, how important is it to recognize human needs in order to improve information security from an organizational perspective?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

10. How important is it to have programs focused on teaching people how to learn instead of teaching specific facts or instructions?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

11. Due to the wide spread use of information technology and associated security concerns, is it important to have a knowledge environment?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

12. To what degree do you believe knowledge has become the key resource to be managed?

- Extremely High
- High
- Average
- Low
- Extremely Low

13. To what extent do you feel new information security technological innovations or improvements are causes for social problems?

- Extremely High
- High
- Average
- Low
- Extremely Low

14. How important is it to respond to social concerns discovered after new information technology innovations have been implemented?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

15. How important is it to have methods and procedures in place that explain how to manage the increasing amount of information?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

16. In order to get the most benefit, how important is it to address people, process and technology resources in policies?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

17. How important is it to give up/terminate existing programs/projects in order to have resources for new initiatives?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

18. How important is it to have innovation initiatives tied to the business strategy?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

19. How important is it to have objectives that guide strategic planning?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

20. How important is it to respond to the differing views, thinking, and characterization of actions given access to so many different information types and sources?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

21. How important is it to factor in social impacts early when developing new business ventures?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

22. How important is it for employees to be included in information security manager discussions aimed at rationalizing the affects of information security controls that may affect profit making activities?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.

23. To what degree has the Federal Information Security Management Act (FISMA) of 2002 standardized the methodology used to provide consistency in federal government information security programs?

- Extremely High
- High
- Average
- Low
- Extremely Low

24. How important is it to appoint chief information officers and assign them responsibility for information security management?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

25. How important is it to direct use of commercial products to institutionalize standardization and reduce duplication?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

26. How important is it to have policies which assign specific and detailed information security management responsibilities to organizational leaders?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

27. To what degree do you believe FISMA's policies ignore the constraints placed on smaller segments of society or organizations?

- Extremely High
- High
- Average
- Low
- Extremely Low

28. How important is it to enact information security controls incrementally so the cultural change impacts will not be so dramatic?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

29. How important is it to classify information so it can be protected during information sharing and collaborative sessions?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

30. To what degree do you believe over classification of information hampers information sharing?

- Extremely High
- High
- Average
- Low
- Extremely Low

31. How important is the use of process, data, and technology standardization and simplification techniques (instead of fixed controls) in meeting information security goals?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

This section is designed to gauge your thoughts on the effectiveness of certain governance approaches used to reduce information security risks in organizations.

32. How important is it to have a governance framework that balances the need for information technology and governance rules?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

33. To what degree do you feel there is a lack of balance and transparency in government power sharing with the IT community, business sector and non profit organizations?

- Extremely High
- High
- Average
- Low
- Extremely Low

34. How important is it to regulate open and closed network systems, through governance, to address economic and geopolitical issues?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

35. How important is it for the government to serve as a mediator or enforcer in debates or discussions about information system security governance and regulation?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

36. To what degree do you feel governance processes are weakened because the less powerful entities or minority groups are under represented?

- Extremely High
- High
- Average
- Low
- Extremely Low

37. How important is it to have a strong correlation associated with better IT security outcomes and implemented governing policies (e.g. security outcome improvement is related to specific governing policies)?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

38. How important is it for organizations to remain open to new techniques or methods of governance (new arrangements, organizational patterns & forms of knowledge production)?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

39. To what degree is it important for governing policies to be seen as creating favorable conditions for private enterprises and placing responsibility with citizens/employees to encourage individualism and entrepreneurialism?

- Extremely High
- High
- Average
- Low
- Extremely Low

40. How important is it for individuals to have trust in electronic governance policies, methods, and procedures?

- Very Important
- Important
- Neutral
- Somewhat Important
- Not Important

41. To what degree do you believe weak public sector management, lack of policy making transparency, perceived unfairness in the rule of law, and lack of openness to citizens/employees detract from the effectiveness of governing policies?

- Extremely High
- High
- Average
- Low
- Extremely Low

Curriculum Vitae

SUMMARY

Over twenty six years of communications and electronic systems leadership, management, operations, planning, engineering and integration experience with the U.S. Air Force and Department of Defense (DoD).

CAPABILITIES

Accomplished joint and combined staff leader: Translated command, control, communications, computers and intelligence system vision into actions focused on revolutionizing military affairs for major combat support defense agency, combatant, and combined commands.

Savvy resource manager: Conceived new IT management approaches that overcame resource shortfalls within the execution year and aligned resources with operational priorities. Resulted in several million dollar savings and operational process improvements across functional mission areas.

Strategic IT planner and implementer: Joint Staff Chief Information Officer and Director of Communications who set theater-wide network centric warfare vision. Implemented significant governance, network security, infrastructure, and interoperability improvements.

Knowledgeable IT Professional. Represented sub unified joint and combined service command around the world. Requested presenter at Asian security and network centric symposiums, Korean security and interoperability conferences, and industry technology panel presentations. Led Korean theater security council and annual awareness conference.

Experienced Information Security Leader. Theater-wide enterprise Designated Approval Authority (DAA) for joint and combined communication systems.

Technology innovation visionary: Understands technology and how to develop cost effective solutions and apply them to improve business operations.

ACCOMPLISHMENTS

Accomplished Joint and Combined senior staff leader

- Current Position: Deputy Commander, Defense Information Systems Agency's Global NetOps Command Center. Synchronizing command and control and situational awareness activities of 13 global NetOps centers. Ensures all enterprise data, voice, security, and collaboration services are reliable and protected for supported combatant commanders, services, and defense agencies.

- Senior US Joint Service communications leader and information officer for all US military forces in South Korea (Joint and Combined). Instituted and chaired joint and combined program management and operational requirements planning processes to collect, validated and prioritize multimillion dollar C4I requirements for the command.

- Led the Defense Information Systems Agency's unclassified Data Network Services Branch in executing a 200 million dollar budget for global data network program management, provisioning, sustainment and life-cycle support. Initiated successful reengineering program that improved global data network baseline configuration, management, security, and control.

- Executive Assistant to the Director, Defense Information Systems Agency (DISA). Translated command, control, communications, computers and intelligence system vision into actions focused on revolutionizing military affairs. $5 million dollar savings realized through CONUS-wide mainframe computer operation consolidation and regional processing center development. Guided planning to establish new defensive network operations mission for DoD.

- DISA liaison with the National Security Agency (NSA) to integrate Public Key Infrastructure (PKI) technology into the Defense Message System (DAWIA Certified program position). Working closely with the NSA, led first secure messaging pilot operations for DoD using security certificate and token technology to authenticate, digitally sign and encrypt messages…first hard token PKI in DoD.

Strategic Resource Manager

- Developed and effectively executed Program Objective Memorandum budget to meet mission requirements specified in strategic information resource management plans. Despite budget reductions in the execution year, innovatively restructured contract work force and realigned projects to preclude mission impacts.

- Directly attacking budget shortfalls…directed a review of all communication service contracts with guidance that we would consolidate services to reduce overhead, re-compete contracts with labor rates in excess of our established average, and combine resources across the staff to pay for communication services. Identified over 10 million dollars in potential savings and at the end of the first year a direct 6 million dollars savings was realized for the command.

- Re-structured umbrella contracts to support consolidation of overhead and reduce resource requirement for similar contract personnel skills. Previously, each staff element had separate, but similar contracts for the same services at significantly different prices.

Strategic IT Planning and Implementation

- Conceived a network centric vision for the command and developed an information resource management strategic plan with associated project management portfolios. The plan synchronized information technology projects with approved and validated business requirements across functional lines of authority.

- Oversaw enterprise security requirements development, assessment, and integration efforts to strengthen the command's monitoring, protection, and reaction posture.

- Advised the senior military commander for U.S. Forces Korea on C2 enhancements for improved reliability and survivability that enabled speed of command through parallel planning. Enhancements made significant governance, network security, infrastructure, and interoperability improvements to the theater-wide enterprise.

Innovation through Technology

- Technology infusion….totally rebuilt 2,500 workstation coalition network enterprise, added new collaboration tools, language translation, implemented voice over internet protocol services and a dynamic web portal for improved information sharing.

- Linked with many IT companies to stay abreast of technology changes which could be used to enhance operations. Introduced thin client capabilities into network enterprise to take advantage of its scalability, flexibility, security, less complex management, and reduction in infrastructure expenses.

- Key Joint Service leadership position in DISA implementing the Defense Message System throughout the DoD…introducing X.400 messaging, X.500 directory standards and PKI security.

EDUCATION

- Bachelors of Science, Business Management, Park University, MO, 1981
- Bachelors of Science, Computer Science, Park University, MO, 2001
- Masters of Science, Computer Information Systems, Webster University, 1989
- Masters of Science, National Security Planning, National Defense University, 2004
- Ph.D., Applied Management and Decision Sciences, Walden University, Feb 2011

PROFESSIONAL AND TECHNICAL TRAINING

- Communications-Electronics Officer Training, Biloxi, MS, 1982
- Yonsei University, Korean Language Center, Seoul, Korea, 1994
- Air Command and Staff College, Maxwell, AL, 1995
- Air War College, Maxwell, AL, 2000
- Industrial College of the Armed Forces, Washington, D.C., 2004

DISTINCTIVE AWARDS

- Republic of Korea Air Force Commendation, 1999
- Republic of Korea, Army Chief of Staff Commendation, Feb 2004
- Republic of Korea, Chairman of Joint Chiefs of Staff Commendation, Dec 2006
- Air Force Outstanding Unit Award Medals
- Joint Meritorious Service Medals
- Defense Meritorious Service Medals

SPECIAL QUALIFICATIONS

- Active Top Secret / Sensitive Compartmented Information clearance
- Korean Language Skills: Intermediate (read, write, & speak).

HOBBIES

- Golf