USING PROSPECT THEORY TO INVESTIGATE DECISION-MAKING BIAS WITHIN AN INFORMATION SECURITY CONTEXT

THESIS

Neil J. Schroeder, Capt, USAF

AFIT/GIR/ENV/05D-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/05D-01

USING PROSPECT THEORY TO INVESTIGATE DECISION-MAKING BIAS WITHIN AN INFORMATION SECURITY CONTEXT

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Neil J. Schroeder, B.S.

Capt, USAF

December 2005

AFIT/GIR/ENV/05D-01

USING PROSPECT THEORY TO INVESTIGATE DECISION-MAKING BIAS WITHIN AN INFORMATION SECURITY CONTEXT

Neil J. Schroeder, BS
Capt, USAF

Approved:

/ SIGNED /	16 Dec 05
Michael R. Grimaila, PhD (Chairman)	date
/ SIGNED /	16 Dec 05
Michael T. Rehg, PhD (Member)	date
/ SIGNED /	16 Dec 05
Juan Lopez Jr., MSGT, USMC (Member)	date

Abstract

Information security is an issue that has increased greatly in importance to both industry executives as well as military leadership over the past decade. In this time both practitioner and academic circles have researched and developed practices and process to more effectively handle information security. Even with growth in these areas there has been almost no research conducted into how decision makers actually behave. This is problematic because information security decision makers in the Department of Defense have been observed exhibiting risk seeking behavior when making information security decisions that seemingly violate accepted norms. There are presently no models in the literature that provide sufficient insight into this phenomenon.

This study used Prospect Theory, developed by Kahneman and Tversky, as a framework to develop a survey in an effort to obtain insight into how decision makers actually behave while making information security decisions. The survey was distributed to Majors in the Air Force who represented a sample of likely future information security decision makers. The results of the study were mixed, showing that prospect theory had only limited explanatory power in this context. The most significant finding showed that negatively connotated decision frames result in significantly more risk seeking behavior. These results provide some insight into potential decision maker behavior and more importantly highlight the fact that there are biases in information security decision making. As such, more research is necessary to investigate this phenomenon before future prescriptive approach development.

Acknowledgements

I would like to extend my thanks to my committee members, Dr. Michael Grimaila, Dr. Michael Rehg, and MSGT Juan Lopez for without their assistance and insight this effort would not have been possible. I would also like to acknowledge and thank Dr. Daniel Kahneman for taking time from his schedule to mentor an aspiring academic. Next I want to express my appreciation to the entire IRM faculty especially Lt Col Summer Bartczak and all of my GIR06M classmates for help and understanding during difficult personal circumstances. Without the compassion shown by everyone my experience at AFIT would have been infinitely more difficult. I am truly a better person for having known everyone here. May our paths cross again.

Even though they are too young to realize any better, my kids provided all the right distractions that helped me keep my perspective and sense of humor throughout this journey. I save my most important acknowledgement for my angelic wife. She has stood by me through all my trials and tribulations while at AFIT and in life. May God grant me the strength to do the same in her hour of need…

Neil J. Schroeder

Table of Contents

Page

Page

List of Figures

Page

List of Tables

Page

USING PROSPECT THEORY TO INVESTIGATE DECISION-MAKING BIAS WITHIN AN INFORMATION SECURITY CONTEXT

I. Introduction

General Background

A recent US Secret Service Survey revealed that 68 percent of companies had knowingly been victims of a cyber attack in 2004. On average each company had to deal with 86 attacks over the course of the year and in total all attacks accounted for losses of a staggering $150 million dollars (E-Crime Survey, 2005). Perhaps partially in response to this hostile environment information security has dramatically jumped in importance over the last decade. A recent survey of business executives revealed that information security was now the third most important information technology issue compared to 1994 when security was not among even the top 25 concerns (Luftman, 2005).

As most organizations have realized that information security is a problem that must be dealt with, they have set about to determine how to better secure their information systems. There are two fundamental tools advanced for this end, technology and process. As highlighted by the surveyed executives, security technologies have become the number one area for internal development in organizations over all other information technology pieces (Luftman, 2005). Many believe that in order to balance the competing demands of system functionality and security the organization must develop a risk management strategy and implement a process to ensure there is adequate

oversight throughout the organization (Purser, 2004; Tipton and Krause, 2004; Coles and Moulton, 2003). Business executives must then set about leveraging both the promise of new technologies and the details of process against an ever changing security environment.

A quick search of the internet reveals there is no lack of information available on technologies in practice that purport to help an organization improve their information security. Similarly one can easily find any number of books or articles in academia that offer perspective processes for dealing with information security and its associated risks (Karyda, et al. 2005; Karabacak and Sogukpinar, 2005; McAdams, 2004; Cavusoglu et. al, 2004; Posthumus and von Solms, 2004; Stewart, 2004; Koskosas and Paul, 2003; Ranier, 1991) Some of the prescribed risk management or security processes in the information technology area involve specific actors that have various roles in information security management decision making and operations. In general, the organization typically includes a security officer whose job is specifically focused on security operations who reports to and works with a security manager, often someone with other executive roles in the organization (Cazemier et. al, 1999; Purser, 2004; Tipton and Krause, 2004).

Department of Defense Related Background

The Department of Defense is no different than industry in regard to its development of literature on information security. This is evidenced through the a new Global Strike integrating document which states, “An integral part of Global Strike preparation and posturing, IO (information operations) must include measures to protect friendly plans and networks and deny the adversary knowledge of pending operations.”

(GS JIC, 2005). The desire to protect defense networks and the information systems that are also part of them led to the creation of a program called the DOD Information Technology Security Certification and Accreditation Process or DITSCAP. The goal of this process is a more deliberate review of new and current information systems such that all aspects of security are considered against the operational needs for the system. (ASD(C3I), 1997). As in the case of commercial security processes, this is a prescriptive process offering a "how to" for managing security in a complex environment.

The roles in these prescribed processes can be broken down into basic functions. As mentioned above, the literature often highlights two individuals as key to the security process. This is not different in the DOD and the DITSCAP process as there are two individuals who are vitally important in making a decision to accept the risk on an information system and subsequently field it. First is the Certification Authority who is the official

> "responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements." (ASD(C3I), 1997).

Second is the Designated Approving Authority who is the executive level official, "with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk." (ASD(C3I), 1997). The work of the CA and the decision of the DAA will ultimately decide whether a new system is brought on line or an old system continues operations.

In order to carry out the entire process, the DAA will task the CA to complete the myriad tasks throughout the DITSCAP process. The CA carries out a straightforward deterministic process called certification, which entails a comprehensive procedure of walking through checklists, vulnerability scans, and other pre-determined items that validate relative strength or weakness in many different technical and non-technical security areas. After the process is complete, the CA aggregates all the various data and looks at the residual risk to then offer a comprehensive risk acceptance recommendation to the DAA about whether the system should be certified, or approved for full operation. The CA can also recommend certification with supplemental recommendations, or the CA can not issue a system certification based on the perceived security risk it would pose. (ASD(C3I), 1997)

Problem Statement

Not only is it possible for the DAA to completely overrule the CA's certification recommendation because of their residual risk assessment, anecdotal evidence in the field indicates that this is quite frequently done. In practice there is a gap between the residual risk perception of the CA and the residual risk perception of the DAA in making their final accreditation decision. It may be expected and even desirable for there to be some gap as the DAA has more executive level information and thus a different perspective than the security centric CA. However, the question when looking at this process is what drives the gap between CA and DAA residual risk assessment? Fundamentally this question implies another: How does the DAA actually make information security decisions? DAAs who were told they had an insecure system still determined that they should operate the system for various reasons and thus the residual risk was acceptable,

when to the CA the risk was so bad that the system should not be operated under any circumstances. Recently there has been little attention paid to this phenomenon or executive decision making in regards to information technology risk assessment and acceptance that would help us understand why DAAs or other executives may engage in this kind of behavior.

While there is ample research on decision making in scholarly literature there appears to be no one model espoused at this point as a possible descriptor for how decision making happens within an information security context. While countless traits and individual factors likely contribute to the final decision, there are several basic decision making theories that provide a parsimonious view of how decisions are made. One such theory will be explored in greater detail as a possible means to provide a foundation to build upon when researching executive decision making. Prospect theory as developed by Tversky and Kahneman (1979, 1981, 1982, 1992) offers one viewpoint on how decision makers may behave when presented with a risky situation as often faced in the information security realm. This theory will be expounded on in greater detail later.

For an organization like the Department of Defense a wide disparity in security decision making can lead to inconsistent approval of systems and ultimately a more insecure environment. Today there is no guiding paradigm that offers insight into the specific nature of decision making in an information security risk assessment context that would help increase security decision making consistency. In order to better understand DAA decision making in regards to this residual risk assessment, a model must be

developed that will allow for exploration of key factors that could influence the decision process.

Research Questions

This research is the first step in an effort to better understand the gap between CAs and DAAs in the DITSCAP process. In order to answer how decision makers decide in an information security context this research will investigate one specific angle. The purpose of this research is to develop a means to answer the following question: Are there biases in decision making that influence a decision maker in an information security context? An expansion of prospect theory in the coming chapter will develop more detailed research questions and propose several hypotheses as well.

This research will require an extensive literature review of such topics as decision making, risk theory, organizational behavior, and information security. In order to test the basic premises of prospect theory in a controlled setting a survey is then developed. The instrument allows for characterization of each key component of prospect theory to help determine if indeed this decision making model is applicable to information technology as well. The instrument will be developed using accepted methodologies to provide reliability and deal with all threats to validity and other problems typically associated with IS survey instruments. Future executions of the survey can provide a means to further explore the decision making process directly with the DAAs.

Implications

The implications of gaining insight into DAA risk assessment decision making behavior will allow the Department of Defense to understand the value of the DAA as well as the entire DITSCAP process. Since DITSCAP is a prescriptive process it only

offers an idealized notion of how information security decisions should be made. This research focuses on how information security decisions are actually made in practice. This will help reveal if there is a fundamental difference in how people actually make decisions and how the DOD would like the process to happen. Validating the principles of one decision making model will provide a foundation from which other needed research can be accomplished. The results could also provide a baseline for developing IA decision making metrics or measurements that provide quantifiable measures of the consistency of decision making and allow for comparison to expected norms in behavior.

Scope of Research

This study is limited to investigation of decision making through the presentation of a scenario with two choices. It does not attempt to address or collect different demographic information, dispositional characteristics, or other potential research items. As such it is scoped to gain insight into potential bias in information security related decision making under risk rather than to compile a detailed list of factors or develop an all encompassing model of behavior. Further this study will be limited to a sample of Majors drawn from the Air Force Institute of Technology (AFIT) primarily due to time constraints faced by the researcher.

Limitations

A key limitation of this study will be that it uses a survey instrument to ask a group of personnel to imagine themselves in hypothetical situations. As such we are merely measuring behavioral intentions rather than actual behavior. This can provide more inconsistent and less generalizeable results. Another limitation of this study will be its focus only on the Department of Defense. The DOD is a unique organization that may

behave differently than many in industry, thus the generalizability of the model, survey, and subsequent results may be weak. As such this research will only be able to be used as a foundation for future work and may not provide a fully vetted information security decision making model in and of itself.

Summary

This chapter provided a brief background on information security and how organizations are attempting to assess the risk posed by their information systems. Specifically an overview of the DITSCAP process was offered and the importance of the actions of the CA and DAA were explained. This lead to addressing the current problem of the differences in CA and DAA residual risk assessment decision making and the lack of any model to further understand the phenomenon how decisions are actually made in this area. The methodology that this research will use to explore this problem area was addressed. Further the implications of the research for the DoD and the IT community at large were discussed.

The remainder of this research will be structured as follows. Chapter two will provide an in depth literature review of many related disciplines. The review will focus on many academic reference disciplines through peer review journals, books, and government publications. Through this review and analysis this chapter will also present the hypotheses developed for research to help answer the questions proposed. Chapter three will discuss the methodology used to develop and execute the survey. Chapter four will present the survey results. Finally chapter five will discuss analysis in detail and the conclusions reached after executing the survey and will discuss a comprehensive way ahead for this research stream and offer other opportunities for related research.

II. Literature Review

Overview

The literature review conducted for this research focused on identifying any research that might be related to or relevant for information security decision making. Since the issue at hand is the DAA's residual risk assessment, careful attention was applied in searching for any specific studies or references to decision making under risk. Biases and influences on risky information security decision making are likely quite varied and not covered completely by any one reference discipline. As a result, sources were drawn from a wide variety of disciplines including information security, information technology, managerial decision making, organizational behavior, and risk theory.

The primary goal of the literature review was to identify an existing line of research or model that would help explain the observed behavior of DAAs while providing a basis for research into current information security decision making scenarios under risk. The model used for investigation should allow for a parsimonious view of how decisions are made independent of dispositional and organizational factors. If there are inherent decision-making biases in the information security context they can be easily exposed at this level. Further, the model must account for decision making under risk. As defined by Rowe, risk is "the potential for realization of unwanted, negative consequences of an event" (Rowe, 1977). In the DITSCAP process the DAA is directly trying to control and mitigate this potential to the greatest extent possible. In the documentation this is stated explicitly, "The DAA should determine the acceptable level

of risk to protect the system commensurate with its value to the Department of Defense" (ASD(C3I), 1997). Therefore, the author used parsimoniousness and risk coverage to sift through the numerous existing decision making frameworks.

Information Technology Security Management

Since the behavior leading to this research effort was witnessed in the information security context it is logical to start with this area in the literature review. Within it there are many frameworks and methodologies espoused for managing information security and enhancing decision making. This section will draw from the major theories and works in an effort to determine their applicability for use in this research from a vast amount of available material.

There are several authors that develop quantitative methodologies for evaluating different areas of information security. One of the most commonly referenced works in this area is Ranier who examines prevailing risk analysis methodologies. He states that, "Because 100 percent IT security is impossible, managers must evaluate the choice of security measures. In general any security measure or combination of such measures must not cost more than it would cost to tolerate the problem addressed by the measures (Ranier et. al, 1991)." This could lead to a hypothesis that a decision maker's perception is that the actual loss of operational capability due to fielding an IT security measure is much greater in cost than the potential loss due to an IT security issue for an unpatched system.

Ranier states that most measures of IT risk are highly subjective which often makes management skeptical of risk analysis, leading to non-use of the risk analysis for

decision making. As such, he focuses his effort on understanding available literature by reviewing four quantitative (Annualized Loss Expectancy, Courtney, Liverore Risk Analysis Methodology and Stochastic Dominance) and three qualitative (Scenario Analysis, Fuzzy Metrics, and Questionnaires) risk analysis methodologies. He then develops his own hybrid eight step process that is prescriptive in nature (Ranier, 1991).

Similar processes for dealing with risk are also outlined in the Facilitated Risk Analysis Process (Peltier, 2004) and the Operationally Critical Threat, Asset, and Vulnerability Evaluation or OCTAVE developed by Carnegie Mellon University (Alberts et. al, 2003). The National Institute of Standards and Technology, NIST, has also developed their Risk Management Guide for Information Technology Systems. Like the others it outlines a comprehensive set of steps and offers other considerations for developing a sound approach to managing risk and information security (Stoneburner et. al, 2002).

Unfortunately, none of these models deal with any factors that may actually influence the final decision. These models are more valuable in helping a decision maker arrive at point to make their final decision, but it is not very useful in helping to explain how decision makers or DAAs actually then decide what to do. In essence it appears to be geared more towards helping the practitioner community versus enhancing the academic communities understanding of information security decision making. This same can be said about many other works in the security realm that offer specific prescriptive approaches to information security (Tipton and Krause, 2004; Purser, 2004)

The quantitative prescriptive approach that seems to be more practitioner focused is explored in various ways by many others as well. Cavusoglu offers a quantitative

model that is specifically developed for the purposes of helping decision makers evaluate IT security investments (Cavusoglu et. al, 2004). McAdams advocates for the establishment of a CSO and offers a prescriptive quantitative approach for how organizations can deal with information security management, however this effort again includes no discussion of actual decision making (McAdams, 2004). The Information Security Risk Analysis Method is an attempt to maintain an objective quantified piece of analysis coupled with management and staff participation in the process. This process is essentially a survey to key people in the company attempting to accurately judge security risk to the organization. (Karabacak and Sogukpinar, 2005). In the end however this technique only provides a quantitative measure of relative risk and still does not deal effectively with other issues in the risk analysis process or risk based decision making.

Beyond simply offering a quantitative methodology several authors have laid out frameworks that try to help managers function in the information security domain. Posthumus and Von Solms offer a framework for the governance of information security. It is prescriptive and has good background considerations for IT security at large. However it does not deal with how decision makers will handle IT security issues (Posthumus and Von Solms, 2004). Coles and Moulton showed that many organizations had gaps in their risk assessment coverage. One key technique is looking at the business processes above technical threats and vulnerabilities. They offer the Business Process Information Risk Management approach which is another attempt to prescribe an approach based on perceived shortcomings with no content on actual decision making (Coles and Moulton, 2003).

Bandyopadhyay et. al, work to offer a framework for managing IT risk that synthesizes current risk management literature into a four step model of risk identification, risk analysis, risk reducing measures, and risk monitoring. This research extends the model through three levels which move from just the technical application level and brings in organizational considerations and even inter-organizational impacts into the model. IT risk is not merely in the domain of technology but rather business operations. This forces a more holistic view to risk management than has been prescribed in the past (Bandyopadhyay et. al, 1999).

This research is prescriptive in a very general sense. Some attention is paid to risk analysis through synthesizing previous research, but no clear answers are offered or measured as far as factors that influence decision makers. The authors state that, "IS managers must change their way of thinking about risk." Further, managers are encouraged to recognize risk at all three levels, to undergo training in decision theory approaches to risk management, and actively participate in the estimation of their organization's overall IT risk (Bandyopadhyay et. al, 1999). However in the end they do no offer specifics of how current managers may or may not actually approach information security decisions under risk.

Some have focused on the policy aspects of information security. Karyda mentions information, hardware, software, the social system, and procedures as the five key components of information systems that must be dealt with for security. IS security management aims to minimize risk that IS face in there operation and includes planning, implementation, assessment, and audit. This study is drawn from the theory of contextualism in order to take into account the influence that the context has on security

management process. Their case study found that organizational structure or a flexible organization is more beneficial in implementing a security policy. Culture or a coherent organizational culture was more conducive to fielding a security policy. Active participation of management and security awareness program were important as well (Karyda et al, 2004). This is again another study that investigates information security but does not include substantial material on decision making in this environment.

One attempt to deal with information systems security decision making that wasn't quantitative or solely prescriptive in nature used job satisfaction as a reference discipline and translated it into IS security satisfactoriness or concern. This lead to a model that three factors would influence security concern, the potential for abuse in an industry, company specific action taken to minimize abuse, and individual factors such as computer literacy, role or others. Unfortunately the author was unable to demonstrate support for this theory at the conclusion of the research effort (Goodhue and Straub, 1991). Additionally, Straub's effort was focused on end users rather than decision makers. Straub and Welke tried to move into this arena and provided an approach grounded in deterrence theory and Straub's earlier unsupported work. This work offers a several phase model that assumes a deterministic path leading to a decision point that is clearly laid out. No time is spent further analyzing how the decision maker might weigh their information security risks (Straub and Welke, 1998).

Stewart offers the idea that it is difficult to calculate a specific level of risk in information security since reporting it is voluntary and haphazard at best. Further, the process is "infinitely reflexive" in an always evolving defense and attack environment. He states that risk must be realistically presented because there is a tendency for IT

security personnel to overestimate risk such that the organization spends too much time trying to remediate risk as well as decreasing productivity because of burdensome security measures. Risk compensation theory highlights the fact that over reliance on one security mechanism may actually increase security incidents rather than decrease them. "Because security professionals live and breathe security, their goal for the level of acceptable risk does not match the company's perception of the acceptable level of risk" (Stewart, 2004). Perhaps then DAA behavior is only a reflection of society in the CA's over cautious eyes.

The information security community has begun to transition its thinking to integrate other theories into their work to help mature the community. Koskosas and Paul effectively brought in other theory by their use of goal setting theory in the context of information security. Their case study research provides evidence that trust, culture and risk communication and their interaction can affect the level of security goal setting within an IT department inside a larger organization (Koskosas and Paul, 2003). This research validated the fact that social characteristics are likely important when considering IT security issues, just as they are in many other cases. Unfortunately for the purposes of the current effort, this research focused on IT departments behavior rather than the decisions made by executives when presented information by IT departments.

Some authors have even suggested that traditional risk analysis in its more narrowly focused quantitative engineering mindset may no longer apply. They advocate for a more comprehensive holistic approach that takes into account the entire spectrum of issues that affect the IT world using the domains of science and other issues centered in areas such as politics, economics, sociology, and others. (Gerber and Von Solms, 2005).

However, this work only suggests breaking out of a traditional mindset without offering concrete advice for a way ahead. It is important nonetheless to see this as the beginning of genuine efforts to mature the body of knowledge as this work is attempting as well.

Like Straub previously, Stanton characterized actual end user behavior and its impact on security (Stanton et. al., 2005). Other end-user research has focused on the development and application of the technology acceptance model. Davis's original concepts of perceived usefulness and perceived ease of use have been expanded upon in numerous ways (Davis, 1989; Venkatesh et. al, 2003; Qingxiong and Liping, 2004). However, all of these efforts focus on how users respond to or perceive technology and are not necessarily applicable to managerial decision making in an information security context.

When looking at the information security related literature it is apparent that this is a difficult subject still somewhat in its infancy. The difficulty in measuring aspects of security are mentioned by numerous authors (Goodhue and Straub, 1991; Posthumus and Von Solms, 2004). This idea has been further accentuated by some who state that, "Risk analysis methods that use intensive quantitative measures are not suitable for today's information security risk analysis." (Karabacak and Sogukpinar, 2005) Several studies have even mentioned explicitly that more research must be done in the area of risk and information security (Straub and Welke, 1998; Bandyopadhyay et. al, 1999). As a result of this immaturity, the literature review must be expanded into other areas in order to help provide a foundation for how decision makers behave under risk in information security situations.

The information security literature above shows two areas of strength in current research efforts. First there have been very robust efforts in developing a prescriptive approach for managing information security and how to make decisions in this area. As the field of information security is relatively new compared to other disciplines this is certainly an important area that requires much background. Second, current research efforts have explored end user issues from acceptance of technology to security behavior at some length. Again the information technology discipline requires this kind of research to be done as well. However, neither one of these areas offers insight into actual decision maker behavior in information security situations. Further maturation in this discipline, especially the development of prescriptive approaches to security will necessitate investigation of how information security decision makers actually behave. Without this understanding future prescriptive approaches may not "get it right."

Decision Making

As there are no well developed descriptive models or frameworks for decision making in information security literature this effort looks to other established reference disciplines for insight. When trying to develop a decision-making model there are three basic approaches to take as outlined by Bell, Raiffa, and Tversky. First is descriptive, which is concerned with how and why people think and act the way they do. Second is normative, which is empirical in nature and deals with an idealized super rational intelligent person who thinks and acts as they should. Third, prescriptive studies such as subjective expected utility tell us what an individual should do and offer a great deal of

pragmatic value. (Bell, Raiffa, and Tversky, 1988). This research effort is an attempt to develop a descriptive model that explains why DAAs have behaved in the way they do.

There are many decision making works that provide basic insights into how anyone may make decisions that could be used for the development of a descriptive model. March's primer on decision making has a great summary of many different facets of decision making as they may apply to this work. His work covers various decision making theories including limited or bounded rationality, rule following, and multiple actor theories for how decisions are made (March, 1994). Rowe and Boulgarides offer both a four factor model of decision making that includes task demands, organizational influences, personal needs, and environmental forces (Rowe and Boulgarides, 1992). Organizational behavior works take a different look at behavior and study how the system of the organization works and influences its decision making (March and Simon, 1993; Cyert and March 1992).

Several works develop specific effects on decision making that are related to this research. A competency trap biases the decision maker against changing the status quo they have settled into through learning processes and positive feedback loops (March, 1993) This theory has been expanded into something called the hot stove affect which states that biases against new and risky alternatives may be less properties of individuals, organizations, or cultures than of competitive selection and reproduction themselves (Denrell and March, 2001). Another study showed that there is a tendency for decision makers to escalate commitment above and beyond what would be warranted by the objective facts of the situation. External justification will lead decision makers to commit

in an effort to prove they were right when facing an external threat or evaluation (Staw, 1981).

Unfortunately, neither individual decision making theories, specific effect research, nor organization theories can totally account for individual behavior under risk. Additionally some of the above theories by themselves are very broad and would jeopardize the parsimoniousness requirement for this study. These works do form the foundation for works that have narrowed their focus of study to how individuals behave in risky situations. For this reason the literature review will now focus on research that is specific to decision making under risk to meet the necessary requirements for the study.

Decision Making Under Risk

Many studies investigate individual facets or influences on decision making under risk. One study investigating this topic fused the personality trait focused Five Factor Model of Extraversion, Neuroticism, Hostility, Lack of Conscientiousness and Openness to Experience with decision making under risk (Lauriola and Levin, 2001). They found that in decision making to avoid a loss personality factors were not statistically significant, but when making a risk decision to achieve a gain low Neuroticism (emotionally stable) and high Openness to Experience were significant predictors of who would make a decision with a higher amount of risk. Personality factors aside males took more risks than females and older people took less risk for gains but more risks to avoid loss (Lauriola and Levin, 2001).

MacCrimmon and Wehrung investigated the relationships between risk taking propensity and a variety of socio-economic characteristics. Among their many findings they found that large organization executives may be more risk averse than their

counterparts in small organizations. They found that the more successful the individual the more inclined they were to take risks probably in a view that risk taking translated into success. Higher individual maturity also led to higher risk aversion and less risk taking behavior (MacCrimmon and Wehrung, 1990).

Kahneman and Lovallo offer several unique ideas. They emphasize the idea of loss aversion. This principle states that losses and disadvantages are weighted more than gains and advantages such that it favors inaction over action and the status quo over any alternatives because the disadvantages of these alternatives are evaluated as losses and are subsequently weighted more than the advantages (Kahneman and Lovallo, 1993). They also offered the idea of the inside view and the outside view. The inside view is generated by focusing on the case at hand, by considering the plan and the obstacles to its completion, by constructing scenarios and by extrapolating current trends. The outside view ignores the details of the case at hand and focuses on the statistics of a class of cases chosen to be similar in relevant respect to the present one. The inside view is often wrong but is still preferred in decision making. The inside view is often overly optimistic: 80% of entrepreneurs rated their chances of success at 70% or better when in reality it was only 33% (Kahneman and Lovallo, 1993).

In a study of risk and decision making on commercial lending, McNamara and Bromiley discovered that organizational factors substantially influence managers' assessments of risky decisions. They also found that standardization of the process did not increase or decrease a manager's risk assessment. Their research also underscored support for the "Fads and Fashion" effect. That is the more "excitement" around a particular industry, the more likely the managers were to underestimate risk. They did

not find support for the idea that more poorly performing firms tend to take more risks (McNamara and Bromiley, 1997).

There are numerous other findings and studies of interest when investigating decision making under risk. Decision makers become more risk averse when they expect their choices to be reviewed by others (Tetlock and Boettger, 1991). There may be behavioral biases in risk management including regret bias (sunk cost, house money), overconfidence, statistical biases (extrapolation, disaster myopia), group think and herding (Rizzi, 2003). There is a positive correlation between the level of risk taking behavior and the managers position in organizational hierarchy while there is no significant correlation between organizational factors and risk taking (Noy and Ellis, 2003). Jia builds on previous efforts and offers a detailed break out of mathematical modeling of perceived risk (Jia, 1999). Because managers are typically in a higher position attained through previous success, they tend to have the perception that their risk taking in previous endeavors has served them well. They tend to think that they can control what appears to be a process of chance. This tends to make managers somewhat more prone to take risks than someone else might be. Also there is societal pressure on managers to behave in this manner as they are expected to make things happen and take good risks to do so. (March and Shapira, 1987) Further, no matter how significant the potential affect, outcomes with low probabilities tend to be ignored. (March and Shapira, 1987).

There is some degree of contradiction between different studies as well. Smidts found that decision makers are intrinsically risk seeking. He found that risk attitude and strength of preference (two factors in hypothesis of intrinsic risk attitude) are to

distinctive constructs (Smidts, 1997). This is contrasted by SP/A Theory and Venture Theory which predict decision makers to be rarely risk seekers (Lopes, 1987; Hogarth and Einhorn, 1990). This conflict is highlighted by the feeling that there is not a perfect way to characterize risk behavior and a lack of full understanding of possible interactions between task characteristic and individual traits. (MacCrimmon and Wehrung, 1990; Tversky and Kahneman, 1992; Lauriola and Levin, 2001). As such, any effort in this study is recognized as not a perfect representation of DAA information security risk behavior, but rather an initial attempt at explaining behavior.

One item that appears many times in decision making under risk literature is the idea of the context that the decision is made in. This is often referred to framing the decision as well (March, 1994; Kahneman and Tversky, 1986). Individual risk preferences in a given situation are not stable, but rather they are strongly influenced by normatively irrelevant changes to the context of judgment (Erb et. al, 2002). Biasing participants with certain types of content before exposure to risk related issues can affect their level of risk seeking behavior. Further the effects can be strong and most participants were unaware of the influence of priming unless their attention was specifically drawn to it (Erb et al., 2002). This theme is reinforced in several earlier works on context dependent risk taking that stated when outcomes are good humans are risk averse but when possible outcomes are poor humans tend to be risk seeking (Kahneman and Tversky, 1979; March and Shapira, 1987).

Some state risk preference varies with context that being primarily influenced by the current focus of the decision maker. In regards to risk the most common focus is success from subjective failure. This line of thinking translates into a risk behavior of

avoiding risk when in or near a successful state and when in or near an unsuccessful state there is a tendency to take more risks (March and Shapira, 1987). Tversky and Simonson highlight the fact that people often do not have a global preference order and as a result they use the context they are in to identify the most attractive option (Tversky and Simonson, 1993). This is counter to the traditional theory of value maximization that assumes that a decision maker will chose the option of highest value when presented with valued options in a given set of alternatives.

The relative attractiveness of one risky option compared to another often depends on the presence or absence of a third option. This is called tradeoff contrast which is broken into background and local contexts. Background context is important because it leads to a higher likelihood of a certain action. Local Context dictates that the "market share" of an option can actually be increased by enlarging the offered set. That is, when presented with a third less appealing option more people would chose the most attractive option than when just two items were present (Tversky and Simonson, 1993).

Tversky and Simonson also cover the concept of extremeness aversion. That means that disadvantages loom larger than the corresponding advantages. As a consequence, options with extreme values within a set of alternatives will be relatively less attractive than options with intermediate values. Compromise is the idea that when faced with extreme options on each end people will tend to chose an option somewhere in the middle of the two presented options. Polarization implies the gravitation from, or aversion of, one extreme only. There is not extremeness aversion in binary (two choice) options (Tversky and Simonson, 1993).

The above studies allow for parsimonious investigation of risk, but do not in themselves provide a single framework that can be used for investigating the observed DAA decision making behavior under risk. They could perhaps be combined into a new framework that would then allow the ability to look at decision making under risk in information security. However, a key issue that would have to be overcome is determining exactly which factors are more important to include over others, and with some disagreement in some areas the task is even more difficult. However, there is already a model that may explain observed behavior and allow for investigation through research. Many of the previously mentioned concepts are captured in a model called Prospect theory that meets both the requirement of parsimoniousness and is a model of decision making under risk.

Prospect Theory

As mentioned earlier, the model used for investigation should allow for parsimonious view of how decisions are made independent of dispositional and organizational factors. If there are inherent decision-making biases in the information security context they can be easily exposed at this level. Further, the model must account for decision making under risk. In the DITSCAP process the DAA is directly trying to control and mitigate this potential to the greatest extent possible. In the documentation this is stated explicitly, "The DAA should determine the acceptable level of risk to protect the system commensurate with its value to the Department of Defense" (ASD(C3I), 1997). Therefore, this study used parsimoniousness and ability of the model to explain risk based decisions to sift through the numerous existing decision making frameworks.

One theory that clearly meets the above criteria as well as offering potential insight to observed behavior at face value is Prospect Theory as developed by Kahneman and Tversky (Kahneman and Tversky, 1979). This is a descriptive theory that was proposed as an alternative to expected utility theory. The deviations it has from expected utility theory may be particularly useful in exploring the behavior anomalies observed by this study's sponsor. The theory is well supported through research and academic development over the years (Tversky and Kahneman, 1979, 1981, 1982, 1986, 1992). It has also been applied at least in a limited manner in the information technology context although not in directly analyzing managerial decision making under risk (Rose et. al. 2004).

Prospect theory as developed offers a model of decision making that can be conceptualized as in Figure 1. First all possible outcomes are edited and framed by the decision maker. The function of this phase is to, "organize and reformulate the options so as to simplify subsequent evaluation and choice" (Kahneman and Tversky, 1979). After the outcomes are framed and edited, the decision maker evaluates each of the options or prospects and chooses the one with the highest value (Kahneman and Tversky, 1979). The value of each is expressed in terms of a decision weight, π, and outcome value, V (see figure 2). The decision weight is assigned to a given probability of an outcome. The outcome value is a subjective measure of how much that particular outcome is worth to the decision maker (Kahneman and Tversky, 1979).

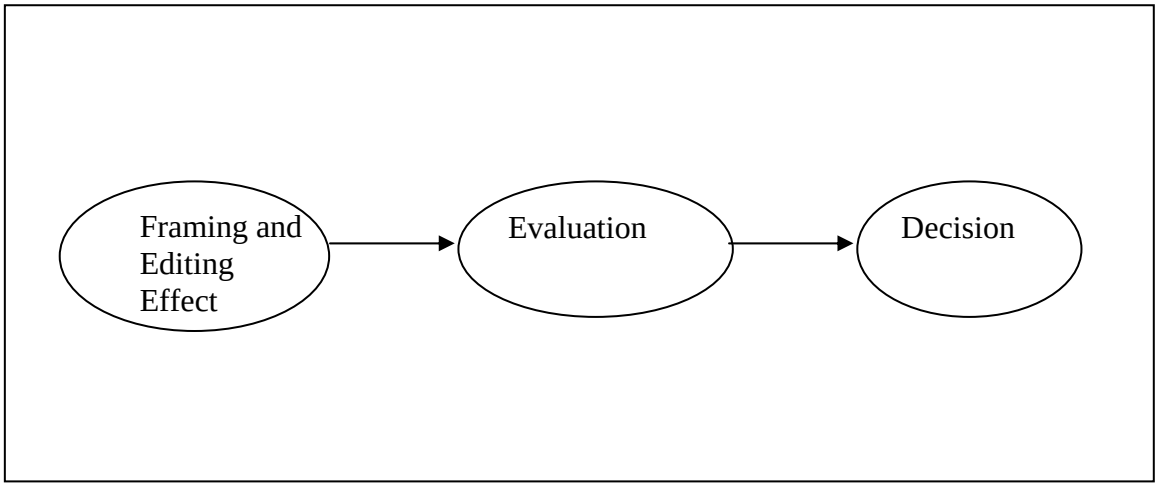

Figure 1 – Prospect Theory Model of Decision Making

The important characteristics of this theory are that value is determined not by overall position but by deviations from a reference point or status quo. That is all outcomes are seen as gains or losses in comparison to a current reference. Secondly gains and losses elicit a certain pattern of decision making behavior under risk such that decision makers are typically risk averse in a gain domain and risk seeking in a loss domain. Additionally, the framing of outcomes can affect the reference point used in evaluation of prospects. The value of prospects also follows an S shaped curve that is concave for gains and convex for losses, with the losses being steeper than gains (Figure 3). It also allows for diminishing losses. These characteristics taken individually or together may be able to be leveraged in explaining the problematic behavior observed by the sponsor of the research.

$$V(x, p\,;\, y, q) = v(y) + \pi(p)[v(x) - v(y)]$$

Figure 2 – Prospect Theory Value Equation

Prospect theory is not without its detractors or competing theories. Weber and Milliman executed two experiments with commuting times and stock choices in order to investigate the if the differences in risky choice behavior could be explained as differences in risk attitude (preferences and personality based) or risk perception (Weber and Milliman, 1997). This study contradicted Prospect Theory's predictions for risk seeking behavior in a loss domain and risk averse behavior in a gain domain. As a result it questions the generalizability of prospect theory outside financial domains. Additional theories such as Security Potential/Aspiration (SP/A) theory, Subjective Expected Utility, and others are not ready to concede to Prospect Theory as the end all for explaining behavior under risk (Bell et. al, 1994).

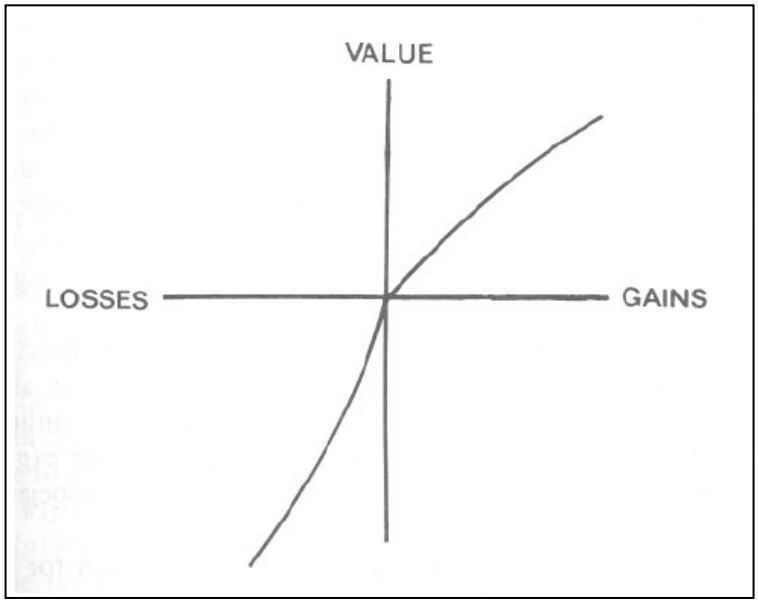

Figure 3 – Prospect Theory Value Function

Besides the previous evidence of success with the theory, the detractors are outweighed by the evidence that using lottery type scenarios to investigate risk in general situations have been found to be more effective than just using psychometric

measurement questions. Penning and Smidts assess the validity of measuring the risk attitude construct through two prevailing measurement approaches. The first measures are derived from the expected utility framework of lotteries and the second are through the use of psychometrics. They found that while psychometric scales were successful in predicting risk attitude variables they did not, in the end, correctly predict behavior (Penning and Smidts, 2000). The expected utility items such as lottery and intrinsic risk measures were effective in predicting actual behavior and had only limited success in predicting risk attitude variables.

Hypotheses

If Prospect theory is to provide a descriptive model for behavior in information decision making, its basic characteristics should be evident in a well designed survey. One way decision makers could be biased is by viewing the security proposition proposed by their personnel as an operational loss. In order to establish both prospect theory in information security and determine if operational loss domains are more poignant, the following hypotheses are proposed:

Hypothesis 1 –
Decision makers are risk averse in gain domains in the information security context.

Hypothesis 2 --
Decision makers are risk seeking in loss domains in the information security context.

Hypothesis 3 –
Decision makers exhibit significantly more risk seeking behavior in operationally framed loss domains than in security framed loss domains.

Prospect theory could also hold descriptive power in the information security context if outcome framing or an explicit shift in the reference point are able to affect risk seeking behavior. The following hypotheses will test these notions:

Hypothesis 4 –
A negative information security outcome frame will result in greater risk seeking behavior than a positive information security outcome frame.

Hypothesis 5a –
Shifting the reference point into a loss domain will result in significantly more risk averse behavior to for losses.

Hypothesis 5b –
Shifting the reference point into a loss domain will result in significantly more risk averse behavior for gains.

Prospect Theory's idea of decision weights and outcome value could also help clarify how DAAs may actually make decisions involving security. Along these lines the following hypothesis is proposed:

Hypothesis 6 –
When presented with situations involving information security and operations, decision makers will tend to give a greater decision weight to operations outcomes.

The final issue in this study deals with how a person's career field background could shape behavior under prospect theory. Since DAAs typically are drawn from line of business or in the military, operational, backgrounds it may be useful to contrast results between operational and non-operational Air Force personnel. The hypotheses are developed from the perspective that the operational personnel will tend to be more risk seeking thus potentially helping to explain observed DAA behavior. While this may not necessarily be the case, for the purposes of hypothesis development one side must be assigned to each sample.

Hypothesis 7a –
Non operational decision makers are significantly more risk averse in information security related gain domains than operational decision makers.

Hypothesis 7b –
Non operational decision makers are significantly more risk averse in information security related loss domains than operational decision makers.

Hypothesis 7c –
Decision makers with an operational background give a greater decision weight to operations outcomes over security outcomes.

Hypothesis 7d –
After a negative shift in the reference point, decision makers with an operational background are more risk averse than non-operational decision makers, in a gain domain.

Hypothesis 7e –
After a negative shift in the reference point, decision makers with an operational background are more risk averse than non-operational decision makers, in a loss domain.

Summary

The literature above demonstrates a relative dearth of prior research into managerial decision making in an information security context. Prospect theory provides one model for investigating this under served area. All the proposed hypotheses seek to use Prospect theory to answer the fundamental question being investigated in this research: Are there biases in decision making that influence a decision maker in an information security context? The following chapters present the results of this effort.

III. Methodology

The Survey Instrument

In order to develop a survey from prospect theory that would investigate information security decision making it was necessary to obtain examples of previously conducted studies in prospect theory. The studies of interest were drawn from the previously validated works of Kahneman and Tversky (Kahneman and Tversky, 1979; Tversky and Kahneman, 1986; Tversky and Kahmenan, 1983). They used the same types of questions in multiple studies which helped validate that the general types of questions they asked did indeed measure risk and risk aversion appropriately. Further these validated studies provided the basis for wording of questions to help ensure that the appropriate constructs were measured.

The approach used in these studies and carried out in this study was to ask scenario preference questions and give two possible choices. One choice always represents a riskless choice offering either a sure loss or sure gain depending on the question. As developed in prospect theory, preference for this option demonstrates risk averse behavior. The other choice is a risky option that presents a certain chance of a greater loss or gain than the sure thing and a certain chance of no gain or loss. As specified in prospect theory, this option represents risk seeking behavior. What changes from question to question throughout the studies is either the context the question is asked in (financial, medical, etc.) or the degree of gain/loss and the percentages involved.

For the purposes of this survey, questions were taken from these works and modified to reflect and information security context rather than financial or medical

contexts as highlighted in the reference works. Wording for each question was chosen to directly mimic the wording of specific questions from previous prospect theory works. The numbers and percentages in each question were also chosen in magnitudes that were represented in questions within the original studies. In each case the wording was only changed enough to change the underlying theme of the question to that of information security. The background presented before the questions was also changed to reflect current security and operations of an information system, rather than a current financial position or as otherwise done in previous prospect theory work. The background also was presented in a manner that framed the decision as an organizational outcome rather than a personal one.

The questions developed for testing the hypotheses proposed in this study fell into several broad categories. In order to test H1, H2, H3, H5, and H7 two sets of questions were developed. One reflected the overall security posture of the information system while the other set reflected the overall operational capability of the system. These two sets of questions were worded exactly the same with the only exception being wording differences to reflect security posture and operational capability. Each of these types of questions also was asked with two different degrees of certainty and magnitude of effect in both a gain and loss frame. This was done in an attempt to strengthen the validity of the overall investigation by using multiple sets of questions for each frame rather than just the results from one question of each type. Two types were chosen to offer more validity while at the same time maintaining a reasonable length for the survey.

Another set of questions was developed to reflect a positive and negative reference frame for a general information security issue. This was done to test H4 and

was very similar to previous prospect theory work that had been done in a medical context (Tversky and Kahnmen, 1986). One question was asked in a positive frame and a second was asked from a negative frame of reference. Both of these questions had the same background and offered two responses that had mathematically equivalent answers and were presented to emphasize either positive aspects of the solution or negative aspects of the solution.

The final set of questions, which tested H6, measured operations and security decision weight together. These questions were developed using previous prospect theory work as a guide, but there were no specific questions that were done previously to reference. As such, a general set of percentages was chosen that was similar to other prospect theory questions. Two questions were developed that emphasized implementing an operational solution at the expense of security and two questions were developed that emphasized a security solution at the expense of operations. Each question again had two responses. One response was to implement the given solution, thereby indicating preference for either operations or security in the given gain or loss circumstance. The other response was to not implement the solution which meant forgoing the gain in one area for no loss in the other area thereby indicating preference for either operations or security as well.

All the questions in the survey were presented immediately after a background reading included in the survey which sought to develop a positive frame for the overall security posture and operations capability of the information system. The questions were also mixed together such that no one type of question repeated and so that questions of all types were as equally separated as possible. The positive and negative framed questions

were intentionally spaced far apart to help mitigate any affect that answering one might have on the other as they are very similar questions. After the first presentation of questions, another background information scenario was presented in the survey that offered a much more negative frame of reference from the security standpoint, while maintaining the same perspective as previously described for operations. The eight questions that specifically targeted security and operations decision making risk behavior were then asked again. This line of questions was developed specifically to target H5 but also could provide some insight into H1, H2, and H3 as well.

The only piece of personal data that was collected was the individual's Air Force Specialty Code (AFSC). While it is entirely possible for people to be new retrainees or have prior enlisted experience in a given area, these areas were not factored in due to the primary focus on Prospect Theory and the desire for survey brevity. They could be included in follow on efforts that may extra more personal factors. This piece of information was essential to test H7. Personal information collection was limited in order to maintain brevity in the survey, provide more simplified results for analysis, and to speed the process of approval for distribution due to time constraints for dispersal. A copy of the final baseline survey is included in Appendix A.

Randomization

To eliminate potential bias of a particular survey, six separate versions of the survey were developed. In an effort to prevent bias from being introduced by the ordering of questions or answers within each survey, a comprehensive randomization scheme was developed. Questions were initially assigned an order in a master survey. As previously mentioned, the baseline order ensured that no type of question was asked

twice in a row or too close together. The baseline attempted to spread all questions as evenly as possible by type to eliminate an order induced bias. Each baseline ordered question was then assigned a group. There were five groups of four questions; gain questions, loss questions, decision weight questions, gain after second scenario, and loss after second scenario. To randomize these groups, a list of all possible permutations of four (24 total) was developed and assigned a number from one to 24. Each group was then assigned a random number between one and 24 that corresponded to the like numbered permutation of four. This ordering was then used for each set of four.

An additional step of randomization was choosing what set of questions to begin each version of the survey with, both in the first set of questions and the set of questions after the second scenario. A one or two was randomly generated in all cases to determine whether each segment would begin with either an increase or decrease question. Depending on the results of this, the placement of all increase or decrease questions would be transposed in each area throughout the survey in order to maintain an ordering like the baseline survey. The set of two verbiage questions were also randomized using a random choice of one or two in order to determine which question came first.

After all the questions were randomized and each of the six survey versions was reordered to reflect the randomizations, the order of responses was randomized as well. To do this a 24 x 6 matrix was develop in Microsoft Excel 2003™. Each question was then randomly assigned a zero or one. Zero indicated that the first response would be A, as specified in the baseline survey, while a one indicated the first response for that particular question would be B, as specified in the baseline. All responses were changed according the randomization matrix and relettered as A and B appropriately. This

provided each randomized survey with a completely randomized order of responses helping to mitigate any bias that may be interjected by presenting the same type of answers in the same order for every question. A summary view of all randomizations completed can be found in Appendix B.

Pilot Survey

A pilot survey was accomplished for this study. The pilot survey instrument was not substantively different than the final baseline survey, as such it is not included. The pilot survey had two primary purposes. The pilot provided a means to test the execution of survey to gather initial insights into timing and potential response behaviors. The survey was also used to solicit feedback on the survey instrument itself in an effort to eliminate poor wording choices, confusion, or other problems that could jeopardize results. The pilot study was not designed to validate proposed hypotheses, as the sample was taken from a different population than that intended in the final survey.

The pilot survey was distributed to 16 students at the Air Force Institute of Technology. The students were from various backgrounds including Medical, Civil Engineering, and Communications/Information career fields. Students held ranks from Senior Master Sergeant to Captain. Due to time constraints, members involved were selected based on direct relationships with author. Thus the sample for the pilot was a non-random convenience sample. Further, the sample in the pilot was not representative of the demographic needed for the study. However, all pilot participants have had graduate level instruction on research methods and have been exposed to various forms of research. Thus this sample still provided a good method of obtaining feedback on questions, wording, and other general issues the survey may have had as well as validating time to completion. The survey was distributed via e-mail to all 16 participants and returned by 10 for a response rate of 62.5 percent. Respondents career fields were as follows: Communication Information Officer – 3, Bioenvironmental

Engineer Officer – 1, Civil Engineering Officer – 3, Communication Information Enlisted – 1, Civil Engineering Enlisted – 1, and Medical Enlisted – 1.

All participants were asked to electronically mark any minor corrections they thought necessary as well as provide detailed comments at the end to include suggestions for improvement, major/minor shortcomings, areas of confusion, or any other issues they may have seen.

Pilot Suggestions

The following are substantive suggestions received after distribution of the pilot survey. This does not include spelling, grammar, or other basic mechanics corrections that were identified. Additionally, positive comments or comments affirming backgrounds, tone, and other areas were not included. Three people did not include any comments. The average time to complete was adjusted to 20-30 minutes from 30-40 minutes. Each comment is preceded with a (C) and the response to each is identified with an (R).

(C) I would caveat questions 15-22 by including the fact that you have new information to base your decision e.g. . "Based on these findings and the new information mentioned directly before question 15 (or something like that), you have two options available of which you must choose one:"

(R) Verbiage was updated to more clearly highlight the fact that those questions were based on the second scenario presented.

(C) Some of the questions didn't seem to be clear or the choice would never seem plausible.

(R) This in regards to a the set of questions that said "Increase system security" and offered an overall decrease in security. Rather than explicitly state increase the security the wording was change to be neutral as to whether security is actually increased or decreased by saying "implement a set of new security measures."

(C) You should add some comments here, like, " End of Survey" and "Thank you for participating in this survey."

(R) END OF SURVEY and "Thank you for your participation in this research effort." Was added to the last page of the survey.

(C) My only suggestion would be to define the difference between security strength and posture…I am not even sure of the difference in terms of networks!

(R) No instance of the word security strength was found in this survey.

(C) Be consistent with either percentages or fractions in the answers and questions.

(R) Percentages and fractions were used in answers in the best possible combinations, mimicking previous prospect theory questions. Most respondents agreed with this format as such it will not be changed.

(C) Use percentages or standardize numerical format. The fractions are not easy to interpret.

(R) Fractions were extensively used in previous prospect theory research as such they will be used in this research effort.

The most significant change resulting from the pilot survey was the rewording of the security posture related questions. Many people were confused by the wording that offered an option to "increase system security." After careful reflection and review, it was apparent that the question scenarios all offered an increase or decrease in a certain percentage so what really needed to be in the answer was merely verbiage reflecting "implementing security measures." This was more applicable to the overall research effort as well, since implementing security measures in the field often comes with uncertain results. Thus, a more realistic verbiage is to "implement several new security measures" and then provide the results of this separately, whether increase or decrease in the system's security posture. Wording in this manner eliminated a scenario where the

question effectively said that increasing the security resulted in the security being decreased, an obvious logical impossibility.

Final Survey Sample and Procedure

This research effort sought to measure, as closely as possible, actual DAA behavior intentions. Due to the complexity of obtaining a sufficient sample size of actual DAAs a sample was used from a similar population. The final survey sample was drawn from Majors (O-4s) attending the Air Force Institute of Technology to obtain various Masters of Science degrees under the auspices of officer Intermediate Development Education (IDE). These Majors are a good sample that can provide generalizability about actual DAA behavior for several reasons. First, all the Majors were competitively selected over their peers to attend this particular IDE in residence school program. This competitive selection often sets the individual on a course that is almost a necessity for promotion into senior officer ranks of O-6 or higher. DAAs are often O-6s or higher, and as such this group of Majors then represents a very likely pool of future DAAs. Additionally, this group of Majors is drawn from a wide diversity of career fields representing all officer careers in the Air Force.

Once selected for intermediate service school in residence programs the Majors have 22 possible options for which school they may attend; however, Air Command and Staff College (ACSC) and the Air Force Institute of Technology (AFIT) present the largest opportunity (AFPC Website, 2005). Officers can indicate preferences, but Air Force policy stipulates that the Air Force will decide where the officer ultimately attends. In the eyes of the Air Force both ACSC and AFIT offer similar end states for the officer that are indistinguishable from the other. Thus, when an officer is assigned to one of

these two programs it is done in a relatively random manner, or at least that is what the Air Force considers the case. As such, for the purposes of this research, the sample in question will be treated as a probability sample because of the random assignment to this program from the larger population of potential future DAAs.

This sample was drawn specifically from those Majors participating in a management focused graduate degree rather than more technical degrees such as physics or an engineering discipline. Based on Air Force career progression there is an increased likelihood that those in the managerial degree program will ultimately be in a senior managerial role in the Air Force, which often has the responsibility of DAA as well. Those in technical degrees are more likely to progress in the science and engineering area which is not of interest in this particular research effort. Approaching the sample in this manner will help strengthen external validity through better generalizability.

The majors chosen for this survey were all participating in a research methods class at the beginning of their second quarter of graduate education. The survey was distributed on the first day of class after approximately 90 minutes of lecture. There were four separate sections totaling 79 participants. The survey was handed out in hard copy by the researcher with instructions on the front page read to everyone. The six different versions of the survey were ordered one after another such that there was a nearly equal distribution of each version. Participation was voluntary however, all were encouraged to complete the survey to help with the research effort. Two individuals chose to take the survey home and did not return it. One individual turned in a completely blank survey for unknown reasons. Seventy six people handed in completed surveys for an overall response rate of 96.2 percent. After collection, all final answered surveys were coded

into Microsoft Excel 2003™. After this was complete, all results were rearranged to reflect the original baseline order of questions and answers for standardized analysis.

Analysis

The analysis of this data was accomplished using Microsoft Excel 2003™, version 11.6355, with its suite of built in capabilities augmented by a statistical analysis program called PHStat, version 1.4, that is commonly distributed with statistics textbooks published by Prentice Hall. Since all results are based on scenarios with two distinctly opposite results, this research will be a combination of large sample tests of hypotheses about a population proportion for single samples and large sample tests comparing two population proportions. Since multiple questions were asked that measured each area, the appropriate question's results were aggregated as necessary for all hypotheses to allow for analysis of the combined data.

The appropriate numbers were developed and used to conduct the necessary hypothesis tests to answer each question. All A answers were coded as zero and all B answers were coded as one. In every case the responses were standardized to mean the same thing. In most cases A specified the risk averse option and B specified the risk seeking option except in the decision weight questions where security favored outcomes were coded as zero and operations favored outcomes were coded as one. Statistical tests of hypothesis were then performed on the aggregated results to see if in the given scenarios the results were statistically different from a null hypothesis of indifference or Ho being $p = .5$. If there were pure indifference in the sample between choices the results would be expected to show that the resultant proportion was .5. If there was a preference for one option or the other, the results should be significantly greater or less. In each

hypothesis test, validity of conditions for a Large-Sample hypothesis test for p are completed as well by ensuring that the interval po +/- $3\sigma_p$ does not contain 0 or 1. Unless noted, all tests satisfied this condition. The other condition for statistical analysis is a random sample, and as mentioned earlier the random assignment of majors to this program will satisfy this requirement.

Reliability calculations were not performed in the data analysis because of the non-applicability of accepted reliability measures for the type of questions offered in this survey. Cronbach's alpha is used in multivariate settings however, Kuder-Richardson formula 20 (KR-20) could be used to determine reliability of dichotomous variables. Unfortunately, due to the structuring of the questions the results from using KR-20 do not provide meaningful results as the coding of the question responses does not always mean the same thing.

IV. Results

This chapter presents the results of analysis of the survey data in regards to how they answer the research questions proposed earlier. The analysis is presented in tables that break out the research question and corresponding hypothesis. The baseline survey questions used for analyzing the particular hypotheses are listed, and then the type of statistical test used is included along with the actual statistical test. Finally, the results of the test are presented along with verbiage that explains what the results mean in basic terms. More complete discussion of results will be included in the next chapter. Analysis was conducted using statistical techniques outlined in *Statistics for Business and Economics* and to a lesser extent Research *Methods for Organizational Studies* (McClave, Benson and Sincich, 2005; Schwab 2005).

Operational and Non-Operational AFSCs were split according to Table 1 for analysis of research question seven and its hypotheses. One individual listed their AFSC as "student" which prevented accurate grouping in any category. In order to maintain more accurate results this record was not used in hypothesis seven. The distribution between operational and non-operational is fairly even. Table 2 provides a quick summary of all results in which hypotheses that were confirmed are bolded. The detailed data collected from the surveys that was normalized to match the base line survey and used for all analysis can be found in Appendix C.

TABLE 1. Job Category of Respondents

Group	Total	Percent of Total	Included AFSCs
Operational AFSCs	35	46.7%	All 11 Series (Pilot), 12 Series (Navigator), and 13 Series (Space and Missile Ops)
Non Operational AFSCs	40	53.3 %	All other AFSCs including 14, 21, 31, 32, 33, 35, 36, 62, and 63 Series.

Table 2. Results Summary

	Results	α	Meaning
H1	**z=-5.85; reject Ho**	**.01**	**Decision Makers are risk averse in Information Security related Gain Domains**
H2	z=.688; fail to reject Ho		Decision makers are not significantly risk seeking in information security related loss domains nor are they significantly risk averse
H3	Z=.2295; fail to reject Ho		Decision makers do not exhibit significantly different behavior between operational outcomes and security outcomes in an information security context loss domain
H4	**Z=3.16; reject Ho**	**.01**	**A negatively phrased information security outcome frame will result in significantly more risk seeking behavior by decision makers than a positively framed similar outcome .**
H5a	Z=.486; fail to reject Ho		After exposure to a negative shift in the reference point decision makers demonstrate no significant change in risk behavior in information security loss domains.
H5b	*Z=-2.014; fail to reject Ho*	*.05*	*After exposure to a negative shift in the reference point decision makers are not significantly more risk averse in gains in an information security context. In actuality this data indicates decision makers are significantly more risk seeking after the shift in reference point!*
H6	**Z=1.950; reject Ho**	**.05**	**Decision makers are significantly more likely to choose operationally favorable outcomes over security favorable outcomes when presented with each in an information security related context.**

TABLE 2 (continued). Results Summary

H7a	**Z=-1.92; reject Ho**	**.05**	**Non operational decision makers are significantly more risk averse in information security related gain domains than operational decision makers.**
H7b	Z=.308; fail to reject Ho		Operational and non operational decision makers do not significantly differ in information security loss domain risk behavior.
H7c	Z=-1.75; fail to reject Ho		Operational background decision makers do not differ significantly from non operational background decision makers in the weighting of operations and security outcomes in information security contexts. *In fact non operational decision makers placed significantly more decision weight on operational outcomes than operational decision makers.*
H7d	**Z=-1.76; reject Ho**	**.05**	**Operational decision makers are significantly more risk averse after exposure to a negative shift in the reference point in information security related gain domains than non operational decision makers.**
H7e	Z=.925; fail to reject Ho		After exposure to a negative shift in the reference point, operational and non operational decision makers do not significantly differ in information security loss domain risk behavior.

TABLE 3. Hypothesis 1 Analysis and Results

Research Question 1: Are decision makers risk averse in gain domains as in the context of information security?	
Hypothesis 1: Decision Makers are risk averse in gain domains in the information security context.	
Corresponding Survey Questions: 1, 5, 8, 11	
Statistical Test 1 – Large Sample Test of Hypothesis about a Population Proportion **Lower Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (indifferent in risk behavior): p = .5 Ha (risk averse thus significantly below .5): p < .5	
Null Hypothesis *p*=	0.5
Level of Significance	0.01
Number of Successes	101
Sample Size	304
Sample Proportion	0.332236842
Standard Error	0.028676967
Z Test Statistic	-5.850101214
Lower-Tail Test	
Lower Critical Value	-2.326347874
***p*-Value**	2.45637E-09
RESULT: Reject the null hypothesis	
CONCLUSION: Research hypothesis confirmed; decision makers are significantly risk averse in general information security gain domains.	

TABLE 4. Hypothesis 2 Analysis and Results

Research Question 2: Are decision makers risk seeking in loss domains in the context of information security?	
Hypothesis 2: Decision Makers are risk seeking in loss domains in the information security context.	
Corresponding Survey Questions: 4, 7, 9, 12	
Statistical Test 2 – Large Sample Test of Hypothesis about a Population Proportion **Upper Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (indifferent in risk behavior): p = .5 Ha (risk averse thus significantly below .5): p < .5	
Null Hypothesis *p*=	0.5
Level of Significance	0.1
Number of Successes	158
Sample Size	304
Sample Proportion	0.519736842
Standard Error	0.028676967
Z Test Statistic	0.688247202
Upper-Tail Test	
Upper Critical Value	1.281551566
***p*-Value**	0.245648562
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; decision makers are indifferent in risk behavior in general information security loss domains.	

TABLE 5. Hypothesis 3 Analysis and Results

Research Question 3: Do decision makers exhibit differing degrees of risk seeking and risk aversion in operationally framed domains versus security framed loss domains?	
Hypothesis 3: Decision makers exhibit significantly more risk seeking behavior in operationally framed loss domains than in security framed loss domains.	
Corresponding Survey Questions: Operational Loss – 4, 7 Security Loss – 9, 12	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Upper Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between ops (p1) and security (p2)): p1 – p2 = 0 Ha (ops (p1) is more risk seeking than security (p2)): p1 – p2 > 0	
Hypothesized Difference	0
Level of Significance	0.1
Group 1	
Number of Successes	80
Sample Size	152
Group 2	
Number of Successes	78
Sample Size	152
Group 1 Proportion	0.526315789
Group 2 Proportion	0.513157895
Difference in Two Proportions	0.013157895
Average Proportion	0.519736842
Z Test Statistic	0.229594678
Upper-Tail Test	
Upper Critical Value	1.281551566
***p*-Value**	0.409203372
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; decision makers are no more risk seeking in operationally framed loss domains than security framed loss domains.	

TABLE 6. Hypothesis 4 Analysis Results

Research Question 4: Can differences in framing through word connotations in an information security problem lead to greater risk seeking behavior?	
Hypothesis 4: A negative information security outcome frame will result in greater risk seeking behavior than a positive information security outcome frame.	
Corresponding Survey Questions: Negative - 2 Positive - 13	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Upper Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between negative (p1) and positive (p2)): p1 – p2 = 0 Ha (negative (p1) is more risk seeking than positive (p1)): p1 – p2 > 0	
Hypothesized Difference	0
Level of Significance	0.01
Group 1	
Number of Successes	56
Sample Size	76
Group 2	
Number of Successes	37
Sample Size	76
Group 1 Proportion	0.736842105
Group 2 Proportion	0.486842105
Difference in Two Proportions	0.25
Average Proportion	0.611842105
Z Test Statistic	3.162335292
Upper-Tail Test	
Upper Critical Value	2.326347874
***p*-Value**	0.000782546
Reject the null hypothesis	
CONCLUSION: Research hypothesis confirmed; decision makers are more risk seeking in negatively framed information security outcomes than the same positively framed outcomes.	

TABLE 7. Hypothesis 5a Analysis and Results

Research Question 5: Will a shift in the decision making reference point alter the preference for given prospects?	
Hypothesis 5a: Shifting the reference point into a loss domain will result in significantly more risk averse behavior to for losses.	
Corresponding Survey Questions: Pre-Treatment Gain – 1, 5, 8, 11 Post-Treatment Gain – 15, 17, 19, 21	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Upper Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between negative (p1) and positive (p2)): p1 – p2 = 0 Ha (after (p2) is more risk averse than before (p1)): p1 – p2 > 0	
Hypothesized Difference	0
Level of Significance	0.1
Group 1	
Number of Successes	158
Sample Size	304
Group 2	
Number of Successes	152
Sample Size	304
Group 1 Proportion	0.519736842
Group 2 Proportion	0.5
Difference in Two Proportions	0.019736842
Average Proportion	0.509868421
Z Test Statistic	0.486759079
Upper-Tail Test	
Upper Critical Value	1.281551566
***p*-Value**	0.313214536
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; A shift in the reference point into a loss domain did not make decision making behavior for losses significantly more risk averse.	

TABLE 8. Hypothesis 5b Analysis and Results

Research Question 5: Will a shift in the decision making reference point alter the preference for given prospects?	
Hypothesis 5b: Shifting the reference point into a loss domain will result in significantly more risk averse behavior for gains.	
Corresponding Survey Questions: Pre treatment Loss – 4, 7, 9, 12 Post Treatment Loss – 16, 18, 20, 22	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Upper Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between negative (p1) and positive (p2)): p1 – p2 = 0 Ha (after (p2) is more risk averse than before (p1)): p1 – p2 > 0	
Hypothesized Difference	0
Level of Significance	0.05
Group 1	
Number of Successes	101
Sample Size	304
Group 2	
Number of Successes	125
Sample Size	304
Group 1 Proportion	0.332236842
Group 2 Proportion	0.411184211
Difference in Two Proportions	-0.078947368
Average Proportion	0.371710526
Z Test Statistic	-2.014081917
Upper-Tail Test	
Upper Critical Value	1.644853627
***p*-Value**	0.977999533
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; A shift in the reference point into a loss domain did not make decision making behavior for gains significantly more risk averse.	

TABLE 9. Hypothesis 6 Analysis and Results

Research Question 6 – Do decision makers place a greater decision weight on operational outcomes or information security outcomes?	
Hypothesis 6 – When presented with situations involving information security and operations, decision makers will tend to give a greater decision weight to operations outcomes.	
Corresponding Survey Questions: 3, 6, 10, 14	
Statistical Test 1 – Large Sample Test of Hypothesis about a Population Proportion **Lower Tail:** Security Outcome (A) Coded as 0. Operations Outcome (B) Coded as 1. Ho (indifferent in decision weights): p = .5 Ha (operations given greater weight): p > .5	
Null Hypothesis *p*=	0.5
Level of Significance	0.05
Number of Successes	169
Sample Size	304
Sample Proportion	0.555921053
Standard Error	0.028676967
Z Test Statistic	1.950033738
Upper-Tail Test	
Upper Critical Value	1.644853627
***p*-Value**	0.025586049
Reject the null hypothesis	
CONCLUSION: Research hypothesis confirmed; When presented with situations involving information security and operations, decision makers will tend to give a greater decision weight to operations outcomes.	

TABLE 10. Hypothesis 7a Analysis and Results

Research Question 7: Does the decision maker's career background have a significant influence on risk behavior in decision making?	
Hypothesis 7a: Decision makers with an operational background are more risk seeking in information security gain domains.	
Corresponding Survey Questions: 1, 5, 8, 11	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Lower Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between non ops (p1) and ops (p2)): p1 – p2 = 0 Ha (non ops (p1) is more risk averse than ops (p2)): p1 – p2 < 0	
Hypothesized Difference	0
Level of Significance	0.05
Group 1	
Number of Successes	45
Sample Size	160
Group 2	
Number of Successes	54
Sample Size	140
Group 1 Proportion	0.28125
Group 2 Proportion	0.385714286
Difference in Two Proportions	-0.104464286
Average Proportion	0.33
Z Test Statistic	-1.919715403
Lower-Tail Test	
Lower Critical Value	-1.644853627
***p*-Value**	0.027446929
Reject the null hypothesis	
CONCLUSION: Research hypothesis confirmed; Non operational decision makers are significantly more risk averse in information security gain domains than operational decision makers.	

TABLE 11. Hypothesis 7b Analysis and Results

Research Question 7: Does the decision maker's career background have a significant influence on risk behavior in decision making?	
Hypothesis 7b: Non operational decision makers are significantly more risk averse in information security related loss domains than operational decision makers.	
Corresponding Survey Questions: 4, 7, 9, 12	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Lower Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between non ops (p1) and ops (p2)): p1 – p2 = 0 Ha (non ops (p1) is more risk averse than ops (p2)): p1 – p2 < 0	
Hypothesized Difference	0
Level of Significance	0.05
Group 1	
Number of Successes	84
Sample Size	160
Group 2	
Number of Successes	71
Sample Size	140
Group 1 Proportion	0.525
Group 2 Proportion	0.507142857
Difference in Two Proportions	0.017857143
Average Proportion	0.516666667
Z Test Statistic	0.308778291
Lower-Tail Test	
Lower Critical Value	-1.644853627
***p*-Value**	0.621254908
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; Non ops decision makers are not significantly more risk averse in information security loss domains than operational decision makers.	

TABLE 12. Hypothesis 7c Analysis and Results

Research Question 7: Does the decision maker's career background have a significant influence on risk behavior in decision making?	
Hypothesis 7c: Operational decision makers demonstrate greater preference for operational outcomes to security outcomes in information security contexts than non operational decision makers.	
Corresponding Survey Questions: 3, 6, 10, 14	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Upper Tail:** Security Outcome (A) Coded as 0. Operations Outcome (B) Coded as 1. Ho (no difference between ops (p1) and non ops (p2)): p1 – p2 = 0 Ha (ops (p1) prefers operations outcomes more than non ops (p2)): p1 – p2 > 0	
Hypothesized Difference	0
Level of Significance	0.05
Group 1	
Number of Successes	61
Sample Size	140
Group 2	
Number of Successes	86
Sample Size	160
Group 1 Proportion	0.435714286
Group 2 Proportion	0.5375
Difference in Two Proportions	-0.101785714
Average Proportion	0.49
Z Test Statistic	-1.759410107
Upper-Tail Test	
Upper Critical Value	1.644853627
***p*-Value**	0.960746062
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; Operational decision makers demonstrate greater preference for operational outcomes to security outcomes in information security contexts than non operational decision makers.	

TABLE 13. Hypothesis 7d Analysis and Results

Research Question 7: Does the decision maker's career background have a significant influence on risk behavior in decision making?	
Hypothesis 7d: After a negative shift in the reference point, decision makers with an operational background are more risk averse than non-operational decision makers, in a gain domain.	
Corresponding Survey Questions: 15, 17, 19, 21	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Lower Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between non ops (p1) and ops (p2)): p1 – p2 = 0 Ha (ops (p1) is more risk averse than non ops (p2)): p1 – p2 < 0	
Hypothesized Difference	0
Level of Significance	0.05
Group 1	
Number of Successes	49
Sample Size	140
Group 2	
Number of Successes	72
Sample Size	160
Group 1 Proportion	0.35
Group 2 Proportion	0.45
Difference in Two Proportions	-0.1
Average Proportion	0.403333333
Z Test Statistic	-1.761430191
Lower-Tail Test	
Lower Critical Value	-1.644853627
***p*-Value**	0.039082809
Reject the null hypothesis	
CONCLUSION: Research hypothesis confirmed; After a negative shift in the reference point, operational decision makers are significantly more risk averse in information security related gain domains than non operational decision makers.	

TABLE 14. Hypothesis 7e Analysis and Results

Research Question 7: Does the decision maker's career background have a significant influence on risk behavior in decision making?	
Hypothesis 7e: After a negative shift in the reference point, decision makers with an operational background are more risk averse than non-operational decision makers, in a loss domain.	
Corresponding Survey Questions: 16, 18, 20, 22	
Statistical Test - Large Sample Test of Hypothesis about p1 – p2 **Lower Tail:** Risk Averse (A) Coded as 0. Risk Seeking (B) Coded as 1. Ho (no difference between ops (p1) and non ops (p2)): p1 – p2 = 0 Ha (ops (p1) is more risk averse than non ops (p2)): p1 – p2 < 0	
Hypothesized Difference	0
Level of Significance	0.05
Group 1	
Number of Successes	74
Sample Size	140
Group 2	
Number of Successes	76
Sample Size	160
Group 1 Proportion	0.475
Group 2 Proportion	0.528571429
Difference in Two Proportions	0.053571429
Average Proportion	0.5
Z Test Statistic	0.9258201
Lower-Tail Test	
Lower Critical Value	-1.644853627
***p*-Value**	0.82273026
Do not reject the null hypothesis	
CONCLUSION: Research hypothesis not confirmed; After a negative shift in the reference point, operational decision makers are not significantly more risk averse in information security related loss domains than non operational decision makers.	

V. DISCUSSION AND CONCLUSIONS

Discussion of Results

As evidenced by the results of the previous chapter, the use of Prospect Theory to model decision making behavior in information security produced mixed results. While it was clear in H1 that decision makers are significantly risk averse in information security gain domains, the results for loss domains in H2 showed no significant risk behavior preference, especially risk seeking as hypothesized. The essence of observed behavior that drove this research effort seemed to show a tendency for risk seeking behavior in domains that presented operational losses while increasing security. Clearly the behavior in this research does not academically confirm this observation. Additionally, the participants in this study did not demonstrate significant difference in risk seeking behavior between operational and security contexts as demonstrated by the results of H3.

H4 provided perhaps one of the clearest possible explanations for any observed risk seeking behavior in information security decisions. The extremely significant results showed that using negative outcome frames will lead to risk seeking behavior. This is a very important finding. It clearly demonstrates that there are circumstances where decision makers risk behavior can be biased by factors outside their control. While the results of H2 showed that decision maker perception of loss domains did not significantly alter decision preference, the negative framing of the outcome did. The next section discusses some of the weakness of the study that may have contributed to this difference in behavior. It is clear that decision making intentions can be significantly affected by the presentation frame of the outcome, when offered negatively. For information security

professionals and decision makers it is thus very important to understand how options presented for decisions are framed in an effort to eliminate this framing bias effect from decision making. While not explicitly stated as a hypothesis, also of note is the fact that there was no statistical difference between operational and non operational personnel when investigating H4. This means that the affect of outcome frames transcended career field background.

Hypothesis 5a and 5b explored how a scenario designed to shift the decision maker's reference point would influence decision making intentions. The negative scenario should have slid the value curve to the left and resulted in even greater risk aversion in most if behavior conformed exactly as prospect theory predicts. In H5a the results did not confirm this behavior. It showed that decision makers were no more risk averse in loss domains than when dealing with a much more positive point of reference. However this result would be expected in this effort as H2 demonstrated that decision makers were not risk seeking in loss domains before the new reference point. As such there would need to be far greater risk aversion after the shift in reference point to produce significant results.

The results of analysis in H5b showed that decision makers are not more risk averse in gain domains after a shift in reference. In fact, it showed that decision makers are actually more risk seeking in gain domains after a negative shift in reference. This is completely contrary to behavior under risk as predicted by prospect theory. At this point, there is little information to indicate why this type of behavior would occur. If this hypothesis were correct it would mean that if a decision maker in practice is exposed to a large negative shift in information security reference point it is likely that decisions made

after that for gains will be risk seeking. This could be a result of the decision maker trying to "get well" by choosing riskier alternatives that offer a chance of greater improvements in security while carrying greater implementation and operational risks. However, more research is necessary in this area to fully understand why the observed phenomenon was such a departure from previously established theory.

H6 offered another interesting significant finding. This hypothesis was an attempt to determine if a decision maker would place greater weight on operational outcomes or security outcomes if forced to choose between the two. As mentioned previously this attempt was an effort to discern how decision weights may be applied as outlined in prospect theory. The results of the research showed that, in general, decision makers are significantly more likely to prefer operational outcomes over security outcomes. This helps to establish the idea that decision makers will tend to place a greater weight on the operational piece versus the security piece when presented with an information security related problem. This is not to say that the weight is so great that it will always outweigh security concerns, but it will impact the final analysis. The fact that operations outweigh security is perhaps intuitively obvious to many people as any information system likely exists to serve some operational purpose important to the organization. It is interesting though that the results were not more significant. This may be because the military environment forces careful consideration between security and operations in all areas not just information security, thus impacting the results.

Hypothesis 7a determined that non-operational decision makers are significantly more risk averse in information security gain domains than operational decision makers. Of note is the fact that this wording is merely a construction of the hypothesis test. The

same test worded in the opposite way, which still yields the same significant results just in the opposite direction is that operational decision makers are significantly more risk seeking that non-operational decision makers in gain domains. However, this does not mean that operational decision makers are risk seeking overall in gain domains, they just happen to exhibit more risk seeking behavior than non-operational personnel. The overall numbers show that they are still risk averse in this area. Hypothesis 7b showed that there was no significant difference between the two groups in loss domains, in contrast to hypothesized behavior.

Hypothesis 7c demonstrated that contrary to the hypothesis, non-operational background AFSC personnel actually placed significantly more decision weight on operational outcomes than operational background personnel. There is insufficient data available in this research effort to explain why this may be the case. The logic behind this hypothesis may be flawed in that operational personnel may actually take a more casual approach to operations than envisioned. Another explanation could involve demand characteristics where operational people tried to be more security conscious because they knew they were under study and non-operational people tried to be more operationally conscious for the same reason. Without more investigation the reasons for this contradiction will not be known.

Hypothesis 7d and 7e dealt with behavior of operational and non-operational personnel after exposure to a negative shift in reference. As hypothesized in 7d, operational personnel were more risk averse in information security gain domains after exposure to the negative scenario than non-operational personnel. However the same behavior difference was not validated in information security loss domains in 7e. The

reason for the significance risk aversion in gains versus no difference in loss domains is not apparent.

The research and hypotheses discussed prevent concluding that prospect theory as described provides a perfect model for describing decision making under risk in information security contexts. It does provide general insights that can be used as a starting point for future research. Decision making is clearly affected by the framing of the problem. Further we know that decision makers will place more weight on operational outcomes than security outcomes. Thus the research has shown that information security decision making is more than just following a prescriptive approach. If a prescriptive approach leads to a decision, one frame could result in a completely different decision than another. An individual's background also clearly influences the decision making process as there are distinct differences between operational and non-operational decision makers, even if they do not directly conform to the espoused hypotheses. This work is an important first step in confirming that there needs to be more attention placed on investigating decision making behavior to perhaps develop a comprehensive descriptive model for how decision making is actually occurring in information security contexts today. From there, prescriptive model development for approaching information security risks will be much more valuable as they will account for reality.

Weaknesses and Limitations

While the assumption of a random sample was explained earlier, it is wholly possible that the sample of majors assigned to AFIT is far from random. There could be a bias between Air Command and Staff College IDE opportunities and AFIT IDE

opportunities. Thus there may have been a purposeful non-random placement of personnel in one program or the other. The sample collected represents an even distribution of career fields, but this may not be the result of randomization it may simply be a by-product of assignment to an IDE program based on some criteria. However, there is nothing that states that there will be a distinction between programs for a specific reason. As such,, the random selection assumption is maintained.

The study was also limited to a degree by the environment in which it was conducted. Since the survey was distributed at the end of each class and presented as the last item of completion before leaving, there is a possibility that adequate thought may not have been given to each scenario. This seems to have been the case somewhat as average completion as observed by the researcher was less then 20 minutes in every case with one individual completing in less than five minutes. This is in contrast to the pilot study, where the average completion time was 25 minutes.

A key limitation of the current study is that it measured behavioral intentions rather than actual behavior. Since the participants were students there was no way to observe them in situations that actually mimicked those that were used to investigate information security risk decision making bias. Intentions do not necessarily correspond directly to actual behavior, so there is a possibility that even when a participant answered in one way they could act the opposite way when faced with a similar scenario in real life. Just as in developing the target sample, it was not possible to measure actual DAA behavior in the allotted time frame. Further, there may be problems with research validity in trying to measure multiple DAAs behavior across widely different contexts. Due to its complexity, information security decision making under risk does not present

easy opportunity for developing standardized scenarios in a laboratory environment that are still realistic and meaningful.

Perhaps the biggest limitation of this effort is the fact that current DAAs were not actually used to investigate DAA behavior. As mentioned before, the difficulty of completing this effort with actual DAAs in the allotted timeframe precluded a direct study. For reasons mentioned above, using a group of likely future DAAs provided a more expedient and efficient approach to investigate information security decision-making behavior. However there is a possibility that this group does not actually reflect DAA behavior in any way. This is due to the fact that these particular individuals may never be DAAs. Further these individuals are earlier in their respective careers meaning there could be any number of effects in the time between this study and the time the individual is a DAA that would influence and shape their decision making processes. Even if DAA comparison assumptions were completely valid or real DAAs were used, the ability to generalize outside the military is very limited. The military is a unique community with a unique set of operational requirements. This environment itself could introduce any number of biases that influence decision makers when compared to their civilian counterparts.

The scenarios themselves may have been a point of potential weakness. While they were structured along previously validated prospect theory work, they may have not accurately captured desired types of scenarios. One reason for this is that the exact wording of the scenarios into an information security decision making context was entirely subjective and at the discretion of the researcher. While words were carefully chosen based on experience, advisor feedback, and pilot response it is still possible that

the wording may not have accurately conveyed the gain and loss domains in an appropriate manner to accurately reflect the constructs being measured in this study. There were no prior studies along these lines that provided a baseline, good or bad, to work from in the development of appropriately worded questions. This weakness could help explain why H2 results were not significant while H4 results were. These questions both presented a risk seeking and risk averse alternative, but their wording and scenario development were entirely different. This disparity should be investigated further. It could be that decision makers are indeed risk seeking in loss domains, but the questions or scenario were worded in such a manner that they did not perceive themselves to be in a loss domain at that time.

The questions in the survey were written in a manner that was general enough that individuals would be able to imagine themselves in that frame of reference without prior experience in that area. However, this generality could also have influenced results. Different participants may have interpreted the meaning of certain words differently than other participants. As a result they may have been making their information security risk based decision in different contexts even though every attempt was made to standardize this context for valid aggregation of results and analysis.

Another area of weakness was that the research was limited in scope and not able to expose all potential biases or may not have been capable of correctly identifying biases as it was limited to a choice of one of two artificially constructed scenarios. This methodology, as outlined in prospect theory, worked well to validate this theory in the arenas of finance and medicine. It has been witnessed to a much lesser extent in

information technology such as in the Rose and Rose study. These situations often were simpler in nature and not necessarily subject to as many influences.

Another limitation with the structuring of questions in the survey was the numbers chosen for each decision area. They were developed to closely mirror previous prospect theory work, but the numbers in the scenarios may have been a confounding variable. Prospect theory outlined that degrees of gain and loss can influence risk decision behavior. However, in this case it was typically skewed at the ends with gain and loss numbers either very low or very high modifying resultant behavior. These types of number situations were avoided in this study. That does not mean that the numbers chosen did not represent some level of extreme on the high end or low end for gains or losses in any participant's opinion. As mentioned, different number combinations were used in an attempt to strengthen generalizability and validity of the final results. However, these different number combinations, if perceived as particularly extreme, could have lead to results that would be inconsistent with situations that are more common and not as extreme.

Another limitation of the study was that the type of data collected limited more detailed analysis through regression and other statistical means to determine if there were other influences into decision making behavior. This does limit the ability to even determine if bias exists in only particular areas or under specific circumstances. For example, collecting detailed demographic data could have revealed differing results by gender, age, or any number of other factors or combination thereof. The research was structured as it was primarily for the purposes of brevity and parsimoniousness to solely investigate the question of existence of bias rather than a detailed analysis of factors that

contribute to bias. Due to the lack of research in this specific subject the effort was scoped to ensure that the basic question of bias existence be answered before structuring more detailed studies.

Future Research

In order to truly investigate any potential biases in DAA information security decision making, the best way ahead may be a case study to directly identify factors by interviewing DAAs before and after security inspections. This effort would allow DAAs to explicitly state how they made decisions. Common factors across many DAAs and many situations could provide the basis for developing a strong model of decision making in information security. This kind of research would be very beneficial and have a high degree of validity, but will take a great amount of time and effort.

Other future research could repeat a similar study with detailed demographics and dispositional characteristics to do factor analysis to determine if there may be influences directly tied to certain characteristics or demographic traits. As outlined in the literature review there have been studies identifying personality traits, demographics such as age, and other areas that have an impact on risk behavior. These may or may not hold true within the context of information security.

Along the same lines, a survey could be used to identify other potential bias factors or items that influence decision making within information security. Questions could be developed to investigate organizational influences such as culture, finances, mission, and others to determine if there are organizational influences. Also a wide variety of other influences could be explored such as trust or others may provide valuable concepts for exploration of information security decisions.

Similar research could be reaccomplished but with a concerted effort to try different types of scenarios. As mentioned in the previous section, there could have been problems with the way the scenarios were worded to reflect gain and loss domains. There may be better ways to do this. In fact this research demonstrated that there are influences on information security decision making, but before taking a similar survey to DAAs more time should be spent developing valid scenarios.

Due to the inclusion and focus only on the military in this research, this approach or any of the additional areas outlined above could be accomplished in a civilian context as well. This may help determine if the phenomenon witnessed here are applicable in every information security related context and if there are any differences. It could very well be the case that the civilian community is even more susceptible to some of the behavioral bias discovered in this research.

Conclusion

This research effort was an attempt to look beyond the prescriptive approaches to managing information security that seem to dominate the literature today. The community of information security professionals may be well off the mark in further prescriptive development if they do not stop to take some time to investigate how decisions are actually being made in the information security arena. As information security involves numerous decisions in risk management, the risk taking behavior of the decision maker must be clearly understood. Unfortunately, decision makers often do not behave in an ideal or prescribed manner. How they handle risk may be consciously influenced by many circumstances that many organizations face including budget

pressures, organizational culture, and other factors. Additionally, risk behavior is likely influenced by a number of factors that the decision maker is not even aware of.

This research was an initial attempt at investigating the subconscious influences that may prime decision makers to behave in certain ways under risk. As mentioned before this effort had mixed results, but its greatest contribution may be the fact that it demonstrated that information security decision makers can be influenced or biased by factors outside of their control. If this is the case, some future research must be accomplished to help understand the phenomenon in greater detail. This is essential in order to develop prescriptive practices taking more into account than just and idealized approach to how a decision maker should handle information security and the risk that it entails. Without more effort along these lines information security is likely to see approaches that may not be feasible in practice. In essence, this jeopardizes further professionalization of the career field of information security. Professionals in this arena must understand how their decision makers actually behave and ensure that they use this knowledge to help make the best information security decisions for their organizations.

Appendix A. Final Survey

Survey Title: Investigating Field Grade Officer Decision Making.

Participation: Your participation in this survey is completely voluntary. However, consider that the greater the participation, the more insightful and useful the data will be for researchers.

Anonymity: We greatly appreciate your participation. All of your responses and information provided in this survey are confidential. No personal information will be collected in this survey.

Contact Information: If you have any questions about the survey, please contact Dr. Michael Grimaila, DSN 785-255-3636 x7399 at **michael.grimaila@afit.edu**.

Survey Instructions:

In this survey, you will be presented with 22 different scenarios that require a choice of two separate decisions.

Please read the background information and then carefully read each question before choosing the answer that most closely reflects the decision you would make.

There are no right or wrong answers, so don't dwell on any one question—just answer what first comes to mind.

Please do not discuss your answers with other students--we don't want your opinions and responses to influence other participants.

ESTIMATED TIME TO COMPLETE: 20-30 Minutes

What is your AFSC ? : _____

BACKGROUND READING:

Following your time at AFIT you are put in charge of an organization in your career field. The organization that you are transferred to uses a particular information system (i.e. a unique software application, a special computer network, a unique hardware setup, etc.) to accomplish its operations. Without this system operating effectively, the organization finds it very difficult to carry out its day-to-day mission. As such, one of your most important
responsibilities is to ensure the continued successful operation of this information system.

Recently, the DoD has issued a policy that all information systems used for operations must be tested to see if there are any problems with the organizations information security posture. The review is to be carried out by a security official from a different organization with a final summary of results presented to you. <u>As specified in DoD policy, the results of the review should be considered by your organization, but the ultimate decision of how to respond to the findings is totally in your hands as the information system owner.</u>

Keeping the above information in mind, please respond to the following questions as if you faced each in the real world.

Consider the information in each question separately from any other questions as they are all unique scenarios.

Circle either option A or B for each of the given questions.

In addition to what you read in the initial background, please read the following description of current operations in your unit and carefully consider it when answering questions 1-14.

CURRENT OPERATIONS DESCRIPTION

Based on your experience and feedback from your staff over the last year, you feel the information system in your unit is operating at a superior level. Furthermore, you feel that current security on the system is very good and perfectly balanced against operations of the system.

QUESTIONS

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *increase* of 10 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 3/4 probability that the system's operational capability will be *increased* by 13.5 percent and a 1/4 probability that no operational capability will be gained.

Your organization expects to have 100 network security incidents (virus outbreaks, hacker attacks, malicious logic, etc.) this year. This is the annual average your organization has experienced over the last five years. You are presented with the following two options that will attempt to bolster network security in your organization of which you must execute one.

A: Implement security plan A which will completely fail to prevent 66 security incidents

B: Implement security plan B, resulting in a 1/3 probability that your organization will prevent all security incidents and a 2/3 probability that your organization will have 100 security incidents.

Your information system was inspected recently and found to contain several areas of concern. This information coupled with the current operations description presented above has forced you to choose one of the following decisions:

A: Implement security measures that increase the system's security posture 15 percent while decreasing its operational effectiveness 15 percent.

B: Do not implement security measures and maintain operational effectiveness while accepting current level of security as adequate.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 10 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 3/4 probability that the system's operational capability will be *decreased* by 13.5 percent and a 1/4 probability that no operational capability will be lost.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *increase* of 25 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 1/2 probability that the system's operational capability will be *increased* by 50 percent and a 1/2 probability that no operational capability will be gained.

Your information system was inspected recently and found to contain several areas of concern. This information coupled with the current operations description presented above has forced you to choose one of the following decisions:

A: Implement operational fixes that increase operational effectiveness 15 percent while decreasing security posture 15 percent.

B: Do not implement operational fixes and operate in a less than optimal manner while maintaining current security level.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 25 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 1/2 probability that the system's operational capability will be *decreased* by 50 percent and a 1/2 probability that no operational capability will be lost.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed 10 percent *increase* in the system's security posture.

B: Do not implement any new security measures. Face a 3/4 probability of a 13.5 percent *increase* in the system's security posture and a 1/4 probability of no increase in security posture.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 10 percent in the system's security posture.

B: Do not implement any new security measures. Face a 3/4 probability of a 13.5 percent *decrease* in security posture and a 1/4 probability of no decrease in security posture.

Your information system was inspected recently and found to contain several areas of concern. This information coupled with the current operations description presented above has forced you to choose one of the following decisions:

A: Implement security measures that increase the system's security posture 60 percent while decreasing its operational effectiveness 30 percent.

B: Do not implement security measures and maintain operational effectiveness while accepting current level of security as adequate.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed 25 percent *increase* in the system's security posture.

B: Do not implement any new security measures. Face a 1/2 probability of a 50 percent *increase* in the system's security posture and a 1/2 percent probability of no increase in security posture.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings, your knowledge of the system, and the current operations description above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 25 percent in the system's security posture.

B: Do not implement any new security measures. Face a 1/2 probability of a 50 percent *decrease* in the system's security posture and a 1/2 probability of no decrease in security posture.

Your organization expects to have 100 network security incidents (virus outbreaks, hacker attacks, malicious logic, etc.) this year. This is the annual average you have faced over the last five years. You are presented with the following two options that will attempt to bolster network security in your organization of which you must execute one.

A: Implement security plan A which will completely prevent 33 security incidents.

B: Implement security plan B which offers a 1/3 probability that all 100 network security incidents will be prevented, and a 2/3 probability that no network security incidents will be prevented.

Your information system was inspected recently and found to contain several areas of concern. This information coupled with the current operations description presented above has forced you to choose one of the following decisions:

A: Implement operational fixes that increase operational effectiveness 60 percent while decreasing security posture 30 percent.

B: Do not implement operational fixes and operate in a less than optimal manner while maintaining current security level.

Before continuing please read the following operations description and make your decisions on questions 15 – 22 carefully considering this new information..

CURRENT OPERATIONS DESCRIPTION

Based on your experience and feedback from your staff over the last year you feel the information system in your unit is operating at a superior level such that no changes are necessary. . However, you recently have had a major virus outbreak that affected your system causing a loss of several hundred man hours of work in your organization. Additionally, a recent criminal investigation reveals that due to poor security someone hacked into your network and downloaded personnel files from a mid level manager's computer. Further, intelligence indicates that there will be heightened cyber attack activity for the next year in response to recent United States geopolitical policies.

QUESTIONS

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *increase* of 10 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 3/4 probability that the system's operational capability will be *increased* by 13.5 percent and a 1/4 probability that no operational capability will be gained.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 10 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 3/4 probability that the system's operational capability will be *decreased* by 13.5 percent and a 1/4 probability that no operational capability will be lost.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *increase* of 25 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 1/2 probability that the system's operational capability will be *increased* by 50 percent and a 1/2 probability that no operational capability will be gained.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 25 percent in the system's operational capability.

B: Do not implement any new security measures. Face a 1/2 probability that the system's operational capability will be *decreased* by 50 percent and a 1/2 probability that no operational capability will be lost.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed 10 percent *increase in* the system's security posture.

B: Do not implement any new security measures. Face a 3/4 probability of a 13.5 percent *increase* in the system's security posture and a 1/4 probability of no increase in security posture.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the

system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 10 percent in the system's security posture.

B: Do not increase the system's security. Face a 3/4 probability of a 13.5 percent *decrease* in the system's security posture and a 1/4 probability of no decrease in security posture.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed 25 percent *increase* in the system's security posture.

B: Do not implement any new security measures. Face a 1/2 probability of a 50 percent *increase* in the system's security posture and a 1/2 percent probability of no increase in security posture.

A security official reviews the security of your organization's information system and presents several areas of concern. Based on these findings and your knowledge of the system, including the new operations information presented above, your organization has two options available of which you must choose one:

A: Implement several new security measures. Realize a guaranteed *decrease* of 25 percent in the system's security posture.

B: Do not implement any new security measures. Face a 1/2 probability of a 50 percent *decrease* in the system's security posture and a 1/2 probability of no decrease in security posture.

END OF SURVEY
Thank you for your participation in this research effort.

Appendix B. Final Survey Radonmization Orders

Translation from Randomization to Master						
Master	**A**	**B**	**C**	**D**	**E**	**F**
1	8	9	7	8	4	11
2	2	2	2	13	2	13
3	6	6	10	14	3	10
4	7	1	5	7	1	7
5	5	12	4	5	7	5
6	14	3	14	3	14	6
7	4	11	8	9	11	9
8	11	7	9	1	9	8
9	9	5	11	12	5	4
10	3	14	3	6	10	3
11	1	4	12	11	12	1
12	12	8	1	4	8	12
13	13	13	13	2	13	2
14	10	10	6	10	6	14
15	18	15	21	22	22	18
16	15	20	16	17	19	19
17	16	21	17	18	18	20
18	19	16	18	19	17	21
19	22	17	19	20	16	16
20	21	18	22	21	15	17
21	20	19	15	16	20	22
22	17	22	20	15	21	15

Start with A or B Randomization

A = 0; B = 1

Question	A	B	C	D	E	F
1	0	0	1	1	0	0
2	0	1	0	0	0	1
3	0	1	1	1	1	1
4	0	0	1	0	0	0
5	1	0	0	0	0	0
6	1	0	1	1	1	0
7	1	0	0	1	0	0
8	1	0	0	0	0	1
9	0	0	1	0	0	1
10	1	1	1	1	0	0
11	1	0	1	1	0	1
12	0	0	1	1	0	1
13	0	1	1	0	0	0
14	1	0	0	1	1	0
15	1	1	1	1	0	1
16	0	0	1	0	0	1
17	1	1	1	1	0	1
18	1	1	1	1	0	0
19	0	0	1	1	0	1
20	0	1	0	0	0	1
21	1	0	1	0	0	0
22	0	0	0	0	1	1

Appendix C. Survey Data

n=	1	2	3	4	5	6	7	8	9	10	11	12
Question	21A	13S	13S	11A	K11M3F	13S	12R	64P	w11f3b	13S	Pilot	14n
1	1	1	1	1	1	1	0	0	1	1	0	1
2	0	1	0	1	1	1	0	0	1	0	0	0
3	1	1	0	1	0	0	0	0	1	0	1	1
4	1	1	1	1	0	0	0	0	1	0	0	1
5	0	0	1	0	0	0	1	1	0	0	1	0
6	0	0	0	0	0	1	0	0	0	0	1	1
7	0	0	1	0	1	0	0	1	0	0	1	0
8	0	0	0	0	0	0	1	1	0	0	1	0
9	1	1	0	1	0	0	1	0	1	0	0	0
10	1	0	0	1	0	0	0	0	0	0	0	1
11	0	1	0	1	1	0	1	0	1	1	1	1
12	1	0	1	0	1	0	1	1	0	0	1	0
13	1	1	1	1	0	1	1	1	1	0	0	1
14	1	1	1	0	0	1	0	0	0	0	1	1
15	0	0	1	0	0	0	0	0	0	0	1	0
16	0	0	0	0	1	0	0	0	0	0	1	0
17	0	0	0	0	0	0	0	0	0	0	1	0
18	1	1	1	1	0	1	0	1	1	1	0	1
19	0	0	0	0	0	0	0	0	0	0	1	0
20	0	0	1	0	1	1	1	0	0	0	1	0
21	0	0	0	0	0	0	0	0	0	0	1	0
22	1	1	0	1	0	1	0	1	1	0	0	1

13	14	15	16	17	18	19	20	21	22	23	24	25
13S4	36p	34M	11H	K11M3L	33S	11F3H	21A	32e	13s	33S	33S4	21M
0	0	0	0	0	1	0	0	0	1	1	1	0
1	1	1	1	1	0	1	1	1	0	1	1	1
1	0	1	0	0	0	1	1	1	0	1	1	0
1	0	1	0	0	0	0	0	1	0	0	0	1
0	0	0	0	0	0	1	0	0	1	0	0	0
0	0	1	1	1	1	0	0	0	0	1	0	1
1	0	0	0	0	0	1	0	1	1	0	1	1
0	0	0	0	0	1	1	0	1	0	0	1	0
1	0	0	0	0	1	1	1	0	1	1	0	1
1	0	1	1	0	0	1	1	1	0	1	1	1
0	0	0	0	0	0	0	0	0	1	0	0	1
1	1	1	1	0	0	1	0	1	1	0	0	1
1	0	1	1	0	1	1	0	0	1	0	0	0
0	1	1	1	1	1	0	0	0	0	1	0	0
0	0	0	0	0	1	1	0	1	1	0	1	1
1	1	0	0	0	1	1	0	1	1	0	1	0
0	0	0	0	0	1	1	0	0	1	0	1	1
1	0	0	0	0	0	1	0	1	1	0	1	0
0	0	0	0	0	0	1	0	0	1	1	0	0
1	0	0	1	0	1	1	0	0	1	0	0	1
1	0	1	1	1	0	0	1	1	0	1	0	0
0	1	1	0	1	1	0	1	0	0	1	0	1

27	28	29	30	31	32	33	34	35	36	37	38	39
13S	33S	K11M3A	31P3	62E	12A	11F3h	13S	14N	33S	21A3	14N	34M3
0	0	0	1	1	1	1	0	1	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1
1	0	1	1	1	1	1	0	1	1	1	1	1
0	0	0	1	1	0	1	1	1	0	1	1	1
1	1	0	0	0	0	0	1	0	1	1	1	1
0	1	1	0	0	0	0	1	0	1	1	1	0
1	1	0	1	0	1	0	1	1	0	1	1	1
0	0	1	1	0	1	1	1	1	0	0	0	0
0	1	0	1	1	1	0	0	1	0	1	0	1
1	1	0	1	1	1	1	1	1	1	0	1	1
1	1	0	0	0	1	0	0	0	0	0	0	0
1	0	1	1	0	1	0	0	1	0	0	0	0
1	1	1	0	1	0	0	1	0	0	0	1	0
0	1	0	0	0	0	0	1	0	1	0	1	0
0	1	0	1	1	1	1	0	1	1	0	0	0
0	0	1	0	1	1	1	0	0	1	0	0	0
0	0	0	1	1	1	1	0	1	1	0	0	0
0	0	0	0	1	1	1	1	1	1	0	1	0
0	1	0	0	0	0	0	1	0	1	0	0	0
1	1	0	1	1	0	0	1	1	0	0	1	0
0	1	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	1	0	0	1	0

41	42	43	44	45	46	47	48	49	50	51	52	53
13M3	32e4	36p	13S	92S	Pilot	13S	64p4	62e3e	32e3g	12R	13s	36p
0	0	0	0	1	0	0	1	0	0	1	0	0
1	0	0	1	1	1	1	0	1	1	1	0	1
0	1	1	1	1	1	1	0	0	0	0	1	1
0	1	1	1	1	0	1	0	1	0	1	1	1
1	1	1	1	1	1	1	0	1	0	0	0	0
0	0	1	1	1	0	0	1	0	0	0	0	0
0	1	0	1	1	0	0	1	1	1	1	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0
1	0	0	1	0	0	1	0	1	0	0	0	1
0	1	1	0	0	1	1	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	1	1	0	0	1	0	1
1	0	0	0	1	1	0	0	0	0	0	0	1
0	0	1	1	0	0	0	0	0	0	1	0	0
0	0	0	0	1	0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	1	0	1	0	1	1
0	0	0	0	1	0	0	1	0	1	1	1	1
1	0	0	0	1	0	0	0	0	0	1	0	1
0	0	0	0	1	0	0	1	0	0	1	0	0
0	0	0	1	0	0	0	0	0	1	0	1	1
0	0	0	0	1	0	0	0	0	1	1	1	1
0	0	0	1	0	1	0	0	0	0	1	0	1

56	57	58	59	60	61	62	63	64	65	66	67	68
11F3h	11F3F	33S3	14N	38M4	13D1A	33S	13S	21r3	21a3	63a3	63a3	14n
0	0	0	0	0	0	0	1	1	0	0	1	1
1	1	0	1	1	1	1	0	1	1	1	0	1
1	1	0	1	0	0	1	1	0	0	0	0	0
0	1	1	0	1	0	0	1	0	0	1	1	1
0	0	0	0	0	0	0	0	1	1	0	0	0
1	1	1	0	0	0	0	0	1	1	0	0	1
0	0	1	0	1	0	0	1	0	0	0	0	1
0	0	0	0	0	1	0	1	1	0	1	1	0
0	0	1	0	0	1	0	0	0	0	0	1	1
1	0	0	0	0	0	1	0	1	0	1	1	1
0	0	0	0	0	0	0	0	0	1	0	0	1
0	1	1	0	1	0	1	0	0	1	0	0	1
0	0	0	1	0	1	1	0	1	1	0	0	1
1	1	1	1	1	1	0	1	1	0	1	1	1
0	0	0	0	0	0	0	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	0	1	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1	1	1	1	1
1	1	0	1	1	1	0	1	1	1	1	0	0
0	0	1	1	0	1	1	1	1	1	1	1	1
1	1	1	0	1	0	0	0	0	0	0	1	1

69	70	71	72	73	74	75	76	Totals
36p/37f	33S	11F3h	13S4	33S3	11M3A	11F4h	11F3h	
1	1	1	1	0	1	1	0	32
1	1	0	1	1	1	0	0	56
0	0	0	1	0	0	0	0	40
1	1	1	1	0	1	1	1	42
0	0	1	0	0	0	1	0	25
0	0	1	0	1	0	1	0	29
1	1	1	0	0	0	1	1	38
1	0	1	0	0	1	0	0	26
1	1	1	1	1	1	1	0	36
1	0	1	0	1	1	1	1	43
0	1	0	0	1	1	0	0	18
1	1	1	1	1	0	1	1	42
0	1	0	1	1	1	0	1	37
1	1	1	0	1	1	0	1	37
1	0	1	0	1	1	1	1	30
1	0	1	1	1	1	1	1	43
1	0	1	0	1	1	1	1	40
0	0	0	0	0	0	0	0	32
1	1	1	1	1	0	1	1	23
1	1	1	0	1	0	1	1	40
1	1	1	0	1	0	1	1	32
0	1	0	1	0	1	0	0	37

Bibliography

Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies? *Decision Sciences, 30*(2), 361.

Ahlbrecht, M., & Weber, M. (1997). An empirical study on intertemporal decision making under risk. *Management Science, 43*(6), 813.

Allison, G. (1971). *Essence of decision: Explaining the cuban missle crisis*. Boston: Little Brown and Company.

ASD(C3I). (1997). Dod information technology security certification and accreditation process (ditscap). In D. o. Defense (Ed.) (Vol. 5200.40).

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437.

Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information technology competence of business managers: A definition and research model. *Journal of Management Information Systems, 17*(4), 159.

Becker, S. A., & Berkemeyer, A. (2004). A case study on a security maturity assessment of a business-to-business electronic commerce organization. *Journal of Electronic Commerce in Organizations, 2*(4), 1.

Bell, D., Raiffa, H., & Tversky, A. (1988). *Decision making: Descriptive, normative, and prescreptive interactions*. Cambridge: Cambridge University Press.

Bhattacherjee, A., & Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage: A theoretlcal model and longitudinal test1. *MIS Quarterly, 28*(2), 229.

Biros, D. P., George, J. F., & Zmud, R. W. (2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly, 26*(2), 119.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 25*(1), 1.

Bozeman, B., & Pandey, S. K. (2004). Public management decision making: Effects of decision content. *Public Administration Review, 64*(5), 553.

Brower, H. H., Schoorman, F. D., & Tan, H. H. (2000). A model of relational leadership: The integration of trust and leader-member exchange. *The Leadership Quarterly, 11*(2), 227.

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R. (2002). Do i really have to? User acceptance of mandated technology. *European Journal of Information Systems, 11*(4), 283.

Burn, J. M., & Szeto, C. (2000). A comparison of the views of business and it management on success factors for strategic alignment. *Information & Management, 37*(4), 197.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating it security investments. *Association for Computing Machinery. Communications of the ACM, 47*(7), 87.

Cazemier, J., Overbeek, P., & Peters, L. (1999). Security management: Itil the key to managing it services. In O. o. G. Commerce (Ed.). London: The Stationery Office.

Cecez-Kecmanovic, D., Janson, M., & Brown, A. (2002). The rationality framework for a critical study of information systems. *Journal of Information Technology, 17*(4), 215.

Cheickna, S., & Wen, H. J. (2002). A conceptual framework for evaluation of information technology investments. *International Journal of Technology Management, 24*(2,3), 236.

Coles, R. S., & Moulton, R. (2003). Operationalizing it risk management. *Computers & Security, 22*(6), 487.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly, 23*(2), 145.

Cyert, R., & March, J. G. (1992). *A behavioral theory of the firm* (Second ed.). Malden: Blackwell Publishers.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user accep. *MIS Quarterly, 13*(3), 319.

Dennis, A. R. (1996). Information exchange and use in group decision making: You can lead a group to information, but you can't make it think. *MIS Quarterly, 20*(4), 433.

Denrell, J., & March, J. G. (2001). Adaptation as information restriction: The hot stove effect. *Organization Science, 12*(5), 523.

Dishaw, M. T., & Strong, D. M. (1999). Extending the technology acceptance model with task-technology fit constructs. *Information & Management, 36*(1), 9.

DOD. (1997). Dod information technology security certification and accreditation process (ditscap). In D. o. Defense (Ed.).

Doll, W. J., Hendrickson, A., & Xiaodong, D. (1998). Using davis's perceived usefulness and ease-of-use instruments for desision making: A confirmatory and multigroup invariance analysis. *Decision Sciences, 29*(4), 839.

Dube, L., & Pare, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations1. *MIS Quarterly, 27*(4), 597.

Dubra, J., & Ok, E. A. (2002). A model of procedural decision making in the presence of risk. *International Economic Review, 43*(4), 1053.

El-Shinnawy, M., & Vinze, A. S. (1998). Polarization and persuasive argumentation: A study of decision making in group settings. *MIS Quarterly, 22*(2), 165.

Erb, H.-P., Bioy, A., & Hilton, D. J. (2002). Choice preferences without inferences: Subconscious priming of risk attitudes. *Journal of Behavioral Decision Making, 15*(3), 251.

Flanagin, A. J., & Waldeck, J. H. (2004). Technology use and organizational newcomer socialization. *The Journal of Business Communication, 41*(2), 137.

Fox, C. R., & Tversky, A. (1998). A belief-based account of decision under uncertainty. *Management Science, 44*(7), 879.

Gerber, M., & Solms, R. v. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16.

Global strike: Joint integrating concept. (2005). In D. o. Defense (Ed.) (1 ed.).

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13.

Hamid Reza, A. (2004). An examination of the role of organizational enablers in business process reengineering and the impact of information technology. *Information Resources Management Journal, 17*(4), 1.

Hamill, J. T., Richard, F. D., & Jack M. Kloeber, J. (2005). Evaluating information assurance strategies. *Decision Support Systems, 39*(3), 463.

Hayward, T., & Preston, J. (1999). Chaos theory, economics and information: The implications for strategic decision-making. *Journal of Information Science, 25*(3), 173.

Hosmer, L. T. (1995). Trust: The connecting link between organizational theory and. *Academy of Management. The Academy of Management Review, 20*(2), 379.

Jia, J., Dyer, J. S., & Butler, J. C. (1999). Measure of perceived risk. *Management Science, 45*(4), 519.

Kahneman, D., & Lovallo, D. (1993). Timid choices and bold forecasts: A cognitive perspective on risk taking. *Management Science, 39*(1), 17.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*(47), 263-291.

Kahneman, D., & Tversky, A. (1982). The psychology of preferences. *Scientific American*(246), 160-173.

Karabacak, B., & Sogukpinar, I. (2005). Isram: Information security risk analysis method. *Computers & Security, 24*(2), 147.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security, 24*(3), 246.

Koskosas, I. V., & Paul, R. J. (2003). A socio-organizational approach to information systems security risks. *International Journal of Risk Assessment and Management, 4*(2,3), 232.

Lally, L. (2005). Information technology as a target and shield in the post 9/11 environment. *Information Resources Management Journal, 18*(1), 14.

Lauriola, M., & Levin, I. P. (2001a). Personality traits and risky decision-making in a controlled experimental task: An exploratory study. *Personality and Individual Differences, 31*, 215-226.

Lauriola, M., & Levin, I. P. (2001b). Relating individual differences in attitude toward ambiguity to risky choices. *Journal of Behavioral Decision Making, 14*(2), 107.

Levy, H., & Levy, M. (2002). Arrow-pratt risk aversion, risk premium and decision weights. *Journal of Risk and Uncertainty, 25*(3), 265.

Lopes, L. L., & Oden, G. C. (1999). The role of aspiration level in risky choice: A comparison of cumulative prospect theory and sp/a theory. *Journal of Mathematical Psychology*(43), 286-212.

Luftman, J., & McLean, E. R. (2004). Key issues for executives. *MIS Quarterly Executive, 3*(2), 14.

MacCrimmon, K. R., & Wehrung, D. A. (1990). Characteristics of risk taking executives. *Management Science, 36*(4), 422.

March, J. G. (1994). *A primer on decision making: How decisions happen*. New York: The Free Press.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science, 33*(11), 1404.

March, J. G., & Simon, H. (1993). *Organizations* (Second ed.). Cambridge: Blackwell Publishers.

McAdams, A. (2004). Security and risk management: A fundamental business issue. *Information Management Journal, 38*(4), 7.

McClave, J. T., Benson, G. P., & Sincich, T. (2005). *Statistics for business and economics* (Ninth ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

McKnight, D. H., & Norman, L. C. (2005). What builds system troubleshooter trust the best: Experiential or non-experiential factors? *Information Resources Management Journal, 18*(3), 32.

McNamara, G., & Bromiley, P. (1997). Decision making in an organizational setting: Cognitive and organizational influences on risk assessment in commercial lending. *Academy of Management Journal, 50*(5), 1063.

Meulbroek, L. (2002). The promise and challenge of integrated risk management. *Risk Management and Insurance Review, 5*(1), 55.

Millet, I., & Wedley, W. C. (2002). Modelling risk and uncertainty with the analytic hierarchy process. *Journal of Multicriteria Decision Analysis, 11*(2), 97.

Molly McLure, W., & Samer, F. (2005). Why should i share? Examining social capital and knowledge contribution in electronic networks of practice1. *MIS Quarterly, 29*(1), 35.

National Institue of Standards and Technology. (2002). Risk management guide for information technology systems: Recommendations of the national institute of standards and technology. In NIST (Ed.) (Vol. SP 800-30).

Nigel, M., Kenneth, K., & Vijay, G. (2004). Review: Information technology and organizational performance: An integrative model of it business value1. *MIS Quarterly, 28*(2), 283.

Noy, E., & Ellis, S. (2003). Risk: A neglected component of strategy formulation. *Journal of Managerial Psychology, 18*(7/8), 691.

Nwachukwu, S. L. S., & Scott J. Vitell, J. (1997). The influence of corporate culture on managerial ethical judgments. *Journal of Business Ethics, 16*(8), 757.

Peltier, T. (2004). Risk Analysis and Risk Management. *The EDP Audit, Control, and Security Newsletter*, 32(3), 1.

Pennings, J. M. E., & Smidts, A. (2000). Assessing the construct validity of risk attitude. *Management Science, 46*(10), 1337.

Philip, G., & McKeown, I. (2004). Business transformation and organizational culture: The role of competency, is and tqm. *European Management Journal, 22*(6), 624.

Pijpers, G. G. M., Bemelmans, T. M. A., Heemstra, F. J., & Montfort, K. A. G. M. v. (2001). Senior executives' use of information technology. *Information and Software Technology, 43*(45), 959.

Politis, J. D. (2003). The connection between trust and knowledge management: What are its implications for team performance. *Journal of Knowledge Management, 7*(5), 55.

Posthumus, S., & vonSolms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638.

Pun, K. F., & Lee, M. K. O. (2000). A proposed management model for the development of strategic information systems. *International Journal of Technology Management, 20*(3,4), 304.

Purser, S. (2001). A simple graphical tool for modelling trust. *Computers & Security, 20*(6), 479.

Purser, S. (2004). *A practical guide to managing information security*. Norwood, MA: ARTECH House.

Qingxiong, M., & Liping, L. (2004). The technology acceptance model: A meta-analysis of empirical findings. *Journal of Organizational and End User Computing, 16*(1), 59.

Ranier, R., Snyder, C., & Carr, H. (1991). Risk analysis for information technology. *Journal of Management Information Systems, 8*(1), 129-147.

Rizzi, J. V. (2003). Behavioral bias: The hidden risk in risk management. *Commercial Lending Review, 18*(6), 2.

Rose, J. M., Rose, A. M., & Norman, C. S. (2004). The evaluation of risky information technology investment decisions. *Journal of Information Systems, 18*(1), 53.

Ross, W. H., & Wieland, C. (1996). Effects of interpersonal trust and time pressure on managerial mediation strategy in a simulated organizational dispute. *Journal of Applied Psychology, 81*(3), 228.

Rowe, A., & Boulgarides, J. (1992). *Managerial decision making*. New York: Macmillan Publishing.

Rowe, W. (1977). *An anatomy of risk*. New York: John Wiley and Sons.

Ryan, S. D., & Harrison, D. A. (2000). Considering social subsystem costs and benefits in information technology investment decisions: A view from the field on anticipated payoffs. *Journal of Management Information Systems, 16*(4), 11.

Schwab, D. P. (2005). *Research methods for organizational studies* (2nd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Sircar, S., Turnbow, J. L., & Bordoloi, B. (2000). A framework for assessing the relationship between information technolgy investments and firm performance. *Journal of Management Information Systems, 16*(4), 69.

Smidts, A. (1997). The relationship between risk attitude and strength of preference: A test of intrinsic risk attitude. *Management Science, 43*(3), 357.

Sopher, B., & Narramore, J. M. (2000). Stochastic choice and consistency in decision making under risk: An experimental study. *Theory and Decision, 48*(4), 323.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124.

Staw, B. M. (1981). The escalation of commitment to a course of action. *Academy of Management. The Academy of Management Review (pre-1986), 6*(000004), 577.

Stewart, A. (2004). On risk: Perception and direction. *Computers & Security, 23*(5), 362-370.

Straub, D., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring system usage: Implications for is theory testing. *Management Science, 41*(8), 1328.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441.

Stoneburner, G., Goguen, A., Feringa, A., (2002). Risk Management Guide for Infromation Technology Systems. National Institute of Standards. SP 800-30.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. *Management Science, 42*(1), 85.

Tallon, P. P., Kraemer, K. L., & Gurbaxani, V. (2000). Executives' perceptions of the business value of information technology: A process-oriented approach. *Journal of Management Information Systems, 16*(4), 145.

Tamura, H. (2005). Behavioral models for complex decision analysis. *European Journal of Operational Research, 166*(3), 655.

Taylor, S., & Todd, P. (1995). Assessing it usage: The role of prior experience. *MIS Quarterly, 19*(4), 561.

Thatcher, J. B., & Perrewe, P. L. (2002). An empirical examination of individual traits as antecendents to computer anxiety and computer self-efficacy. *MIS Quarterly, 26*(4), 381.

Thomson, K.-L., & Solms, R. v. (2005). Information security obedience: A definition. *Computers & Security, 24*(1), 69-75.

Tipton, H. F., & Krause, M. (2003). *Information security managment handbook* (4th ed. Vol. 4). Boca Raton: Auerbach Publications.

Trcek, D. (2003). An integral framework for information systems security managemen. *Computers & Security, 22*(4), 337-360.

Tversky, A., & Kahneman, D. (1986). Rational choice and the framing of decisions. *The Journal of Business (1986-1998), 59*(4), IIS251.

Tversky, A., & Kahneman, D. (1992). Advanceds in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*, 297-323.

Tversky, A., & Simonson, I. (1993). Context-dependent preferences. *Management Science, 39*(10), 1179.

US Secret Service. (2005). 2005 e-crime watch survey. *CSO Magazine*.

Venkatesh, V. (1999). Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS Quarterly, 23*(2), 239.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for dirrections? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly, 24*(1), 115.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view1. *MIS Quarterly, 27*(3), 425.

Venkatesh, V., Speier, C., & Morris, M. G. (2002). User acceptance enablers in individual decision making about technology: Toward an integrated model. *Decision Sciences, 33*(2), 297.

Von Solms, B. (2005). Information security governance: Cobit or iso 17799 or both? *Computers & Security, 24*(2), 99.

Weber, E. U., & Milliman, R. A. (1997). Perceived risk attitudes: Relating risk perception to risky choice. *Management Science, 43*(2), 123.

William, L., Ritu, A., & Sambamurthy, V. (2003). Sources of influence on beliefs about information technology use: An empirical study of knowledge workers1. *MIS Quarterly, 27*(4), 657.

Yang, J., & Qiu, W. (2005). A measure of risk and a decision-making model based on expected utility and entropy. *European Journal of Operational Research, 164*(3), 792.

Yoris, A. A., & Robert, J. K. (2003). What do you know? Rational expectations in information technology adoption and investment. *Journal of Management Information Systems, 20*(2), 49.

Youngjin, Y., & Maryam, A. (2001). Media and group cohesion: Relative influences on social presence, task participation, and group consensus. *MIS Quarterly, 25*(3), 371.

Yu, L. (2002). Risk management in practice. *MIT Sloan Management Review, 44*(1), 9.

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science, 9*(2), 141.

Vita

Captain Neil Schroeder graduated from Hartley-Melvin-Sanborn High School in Hartley, IA in 1994. He attended the United States Air Force Academy, graduating in May of 1998. While at the Air Force Academy he earned a Bachelor's of Science in Political Science and was presented with the Robert K. Smith award for academic excellence as one of the top graduates in the Political Science major. He was commissioned as a Communications and Information officer and subsequently attended Basic Communications Officer Training where he was awarded the distinguished graduate award for top performer in his class.

His first active duty assignment was to Royal Air Force Mildenhall Air Base in the United Kingdom. During his time there he held several jobs, ending the second half of his tour as the Director of the Network Control Center. He was deployed twice to support Operation ALLIED FORCE at Aviano Air Base in Italy, and to Eskan Village in Riyadh Saudi Arabia in support of Operation SOUTHERN WATCH. In August of 2001 he was assigned to Air Intelligence Agency where he worked first in the 690th Intelligence Support Squadron followed by duty in the 33 Information Operations Squadron as a Flight Commander. In August 2004 he entered the Air Force Institute of Technology at Wright Patterson Air Force base to obtain a Master of Science Degree in Information Systems Management. Following his school assignment, Captain Schroeder will be assigned to the J8 (future capabilities) directorate of the United States Strategic Command at Offutt Air Force Base.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
December 2005	**Master's Thesis**	Aug 2004 – Dec 2005

4. TITLE AND SUBTITLE

Using Prospect Theory to Investigate Decision-Making Bias Within an Information Security Context

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Schroeder, Neil, J., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05D-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Marine Forces, Atlantic
Attn: MSGT Juan Lopez
8412 O'Connor Crescent
Norfolk, VA 23503 DSN: 564-7134

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Information security is an issue that has increased in importance over the past decade. In this time both practitioner and academic circles have researched and developed practices and process to more effectively handle information security. Even with growth in these areas there has been little research conducted into how decision makers actually behave. This is problematic because decision makers in the Department of Defense have been observed exhibiting risk seeking behavior when making information security decisions that seemingly violate accepted norms. There are presently no models in the literature that provide sufficient insight into this phenomenon.

This study used Prospect Theory as a framework to develop a survey in an effort to obtain insight into how decision makers actually behave while making information security decisions. The survey was distributed to Majors in the Air Force who represented likely future information security decision makers. The results of the study were mixed, showing that prospect theory had only limited explanatory power in this context. The most significant finding showed that negatively connotated decision frames result in significantly more risk seeking behavior. These results provide insight into decision maker behavior and highlight the fact that there are biases in information security decision making.

15. SUBJECT TERMS
Information Security, Prospect Theory, Decision Making, Decision Theory, Management, Certification and Accreditation, Information Technology, Computer Security, Communications Networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Dr. Michael R. Gramaila (ENV)
U	**U**	**U**	**UU**	110	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4800; e-mail: Michael.Grimaila@afit.edu