IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12708

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Revealing Prospect Theory Bias in Information Security Decision Making

Neil J. Schroeder & Michael R. Grimaila
Air Force Institute of Technology, Wright-Patterson AFB, OH, 45433-7765, P: 937-3636 x4800, F: 937-645-4699,
Neil.Schroeder@AFIT.EDU, Michael.Grimaila@AFIT.EDU

ABSTRACT

It is believed that security management decisions are made with the intent of maximizing the decision maker's utility. In this paper, we examine the influence of biases on information security decision making through Prospect Theory. A scenario-based survey of 78 military officers was conducted and analyzed to identify if there is an underlying source of bias present in information security decision makers.

1. BACKGROUND

The 2005 E-Crime survey administered by the US Secret Service 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 reported attacks accounted for losses of a staggering $150 million dollars (E-Crime Survey, 2005). 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).

A quick literature review reveals any number of books or articles 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; Straub and Welke, 1998, Ranier, 1991). Organization typically include 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).

The Department of Defense (DoD) is no different than industry in regard to its development information security policies. A historical desire to protect its information systems led to the creation of a program called the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Specific to the DoD process are the Certification Authority (CA) and the Designated Approving Authority (DAA). In DITSCAP, the CA conducts security reviews and makes recommendations to the DAA who is the executive charged with determining if the system meets acceptable levels of risk (ASD(C3I), 1997).

The DAA decision is a complicated by the fact that they must carefully weigh the operational impacts and a variety of other factors beyond just the basic security considerations when making their decision. It is entirely possible that even in the face of a CA recommendation not to operate a system a DAA may choose to do so because the operational impacts of not having the system outweigh the residual risk posed by the system in question. The fundamental question then driving this research is "Is there bias in DoD information security decision making?"

2. LITERATURE REVIEW

Until recently, information security in its many forms and management decision making within have received only marginal attention in academic circles. In fact, some bemoaned that fact that no one was really paying attention to security, the IT department included (Goodhue and Straub, 1991; Straub and Welke, 1998). Goodhue and Straub advanced a security model that used satisfactoriness to measure security adequacy perceptions of users and Stanton characterized actual end user behavior and its impact on security (Goodhue and Straub, 1991; Stanton et. al., 2005). Other end user research relating to information technology 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 or security and are not necessarily applicable to managerial decision making in an information security context.

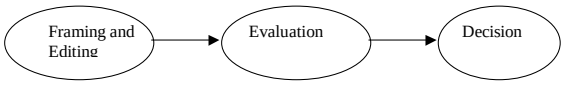
Recent efforts to deal with managerial decision making in information security have been focused on providing prescriptive processes that offer grounded idealized notions of how a manager should cope with information security (Straub and Welke, 1998; Bandyopadhyay et. al., 1999; Bassellier et. al., 2001; Coles and Moulton, 2003; Gerber and Von Solms, 2005; Von Solms, 2005; Pijpers et. al., 2001). There has been little attempt to scientifically determine how decision makers actually behave when presented with an information security decision. That is there are ample normative models of behavior proposed for information security decision making but very few descriptive models explaining actual observed behavior. Decision making literature is well developed and presents several frameworks from which one could choose to use for further analysis and development (Rowe, 1992; March, 1994; March and Simon, 1993; Bell, Raiffa, and Tversky, 1988).

3. THEORY

The model used for investigation should allow for parsimonious view of how decisions are made independent of dispositional and organizational factors. Too many factors will quickly dilute the effectiveness of the model to explain observed behavior. If there are inherent decision-making biases in the information security context they should be exposed at a higher 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 (ASD(C3I), 1997). Therefore, the authors used parsimoniousness and risk coverage 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, 1982). 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 a well supported through research and academic development over the years (Tversky and Kahneman, 1986, 1992). It has also been applied at least in a limited

Figure 1. Prospect theory model of decision making



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 simply 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 choose the one with the highest value (Kahnment and Tversky, 1979). The value of each is expressed in terms of a decision weight, À, and outcome value, *v*. 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 (Kahnment and Tversky, 1979).

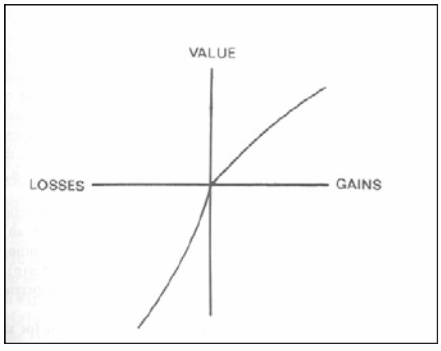
The important characteristics of this theory are that value is determined not by overall position but by deviations from a reference point or status quo. That is all outcomes are seen as gains or losses in comparison to a current reference. Secondly gains and losses elicit a certain pattern of decision 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 and S shaped curve that is concave for gains and convex for losses, with the loss side being steeper than gains (Figure 2). These characteristics individually or taken together may be able to be leveraged in explaining the problematic behavior observed by security officials at the sponsor organization.

4. RESEARCH 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 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.

Figure 2. Prospect theory value function



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 this context if outcome framing or an explicit shift in the reference point are able to affect risk seeking and risk averse 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 5: Shifting the reference point into a loss domain will result in significantly more risk averse behavior to for losses.

Prospect Theory's idea of decision weight's and outcome value could also help clarify how DAA's may actual make decision involving security. Along these lines the follow hypothesis is proposed:

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

5. METHODOLOGY

In order to test the hypotheses, a set of scenarios was developed that in principle replicated earlier work in prospect theory. Rather than build monetary or health related scenarios as previously studied, these scenarios focused on information systems security related items. Several types of scenarios were developed including gain and loss scenarios for system security (4 total), gain and loss scenarios for system operations (4 total), outcome framed scenarios (2 total), and security and operations combined outcome scenarios (4 total). Each scenario presented the opportunity to choose from a riskless prospect offering a sure increase or decrease in the security of the information system or the operational capability of the system and a riskier prospect that offered a chance of greater gain or loss and a chance of no gain or loss. After the first 14 scenarios, a different operations description was provided that was more dire, with system security and operations gain/loss scenarios being presented again exactly as they appeared before. This technique was employed in an attempt to shift the participant's reference point clearly into a loss domain to attempt to ascertain if this would change previously selected decision. As presented these scenarios provide direct insight into decision making behavior in both information system security and operations gain domains and loss domains and help establish the affect of framing on decision making

It is difficult to account for all biases in the development of these utility scenarios however every attempt was made to eliminate potential problems. A gain expectation and loss expectation scenario for both helps control response mode bias (Hershey, et. al., 1988). Also, multiple lottery types are employed including pure loss, mixed, and pure gain to mitigate lottery domain bias (Hershey, et. al., 1988).

The six survey versions were equally distributed to 78 Majors in the United States Air Force, all of whom were attending the Air Force Institute of Technology to obtain a MS in Management. As such, they represent a sample that are likely to be assigned DAA responsibilities.

6. SURVEY RESULTS AND ANALYSES

Table 1 highlights the results of the survey.

The use of Prospect Theory to model decision maker behavior in information security produced mixed results. While it was clear in H1 that decision makers were significantly risk averse in information security gain domains, the results of H2 showed no significant risk behavior preference in loss domains. Additionally, the participants in this study did not demonstrate significant risk seeking behavior in operational or 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. 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 influenced 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. At the very least decision making intention 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 decision are framed in an effort to eliminate this framing affect from decision making.

Hypothesis 5a and 5b, explored how a scenario designed to shift the decision makers 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 moss 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.

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. More research is necessary in this area to fully understand why the observed phenomenon was such as departure from previously established theory.

H6 offered another interesting significant finding. 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 operations versus the security 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 likely impact the final analysis.

Table 1. Summary of research results

	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 negative 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 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.**

7. CONCLUSIONS

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. However, information security 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 information security decision making is more than just following a prescriptive approach. Biases do exist and must be accounted for if organizations wish to have consistent and effective information security decisions. This work is a first step in confirming there needs to be more research devoted to investigating information security decision making behavior biases. From there prescriptive model development for approaching information security risks will be much more valuable as they will account for reality.

8. DISCLAIMER

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

9. REFERENCES

Assistant Secretary of Defense (Command, Control, Communications and Intelligence). (1997). DoD information technology security certification and accreditation process (DISCAP). In DoD (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.

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

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.

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

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

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

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.

Hershey, J., Kunreuther, H., Schoemaker, P. (1982). Bias in assessment procedures for utility functions. *Management Science* (28), 936-954.

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.

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

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

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

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

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.

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

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.

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.

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.

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

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

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

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

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). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*, 297-323.

US Secret Service. (2005). 2005 e-Crime Watch Survey. *CSO Magazine*.

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.

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