December 2006

Looking at Information Security through a Prospect Theory Lens

Hina Arora
Arizona State University

Paul Steinbart
Arizona State University

Benjamin Shao
Arizona State University

Looking at Information Security through a Prospect Theory Lens

Hina Arora
Department of Information Systems
Arizona State University
Box 874606, Tempe, AZ 85287-4606
hina.arora@asu.edu

Paul J. Steinbart
Department of Information Systems
Arizona State University
Box 874606, Tempe, AZ 85287-4606
paul.steinbart@asu.edu

Benjamin Shao
Department of Information Systems
Arizona State University
Box 874606, Tempe, AZ 85287-4606
benjamin.shao@asu.edu

ABSTRACT

Traditional accounts of decision-making under uncertainty have taken the Von Neumann and Morgenstern approach of Expected Utility Theory that considers how decisions under uncertainty *should* be made. This prescriptive model states that, when faced with a choice, a rational decision maker will pick the prospect that offers the highest expected utility. But as has been demonstrated by Kahnemann and Tversky in Prospect Theory, decision-making under uncertainty often deviates from what Expected Utility Theory predicts, largely depending on whether the decision is framed as a gain or a loss. According to their model, choices framed as gains often lead to risk–averse behavior, and choices framed as losses often induce risk-seeking behavior. This paper reviews various theories of decision-making under uncertainty and evaluates the relevance of Prospect Theory in the information security context. An instrument is developed to evaluate relevance, preliminary results are presented, and implications for future research are discussed.

Keywords

Information Security, Prospect Theory.

1. INTRODUCTION

Traditional accounts of decision-making under uncertainty have taken the Von Neumann and Morgenstern approach of Expected Utility Theory (EUT). This prescriptive model states that, when faced with a choice, a rational decision maker will pick the prospect that offers the highest expected utility. However, there is a lot of evidence that decision-making under uncertainty often deviates from what EUT predicts. Prospect Theory (PT) was developed to account for how people actually behave. It is a descriptive model that argues that the choice of decision makers depends on whether the decision is framed as a gain or a loss. This paper evaluates the relevance of Prospect Theory in the context of investments designed to improve information security.

The rest of the paper is organized as follow. Section 2 reviews EUT and PT and discusses the relevance of PT in the investment in security domain. Section 3 evaluates the applicability of PT to decisions concerning investments in security. Section 4 discusses the results of a preliminary experiment. Section 5 concludes the paper.

2. DECISION-MAKING UNDER UNCERTAINTY – THE CASE OF INFORMATION SECURITY

Expected Utility Theory (von Neumann and Morgenstern, 1944) is a normative approach that considers how decisions under uncertainty *should* be made. According to this theory, people should make choices after either explicitly or implicitly calculating an option's likely effect on their final asset position. The theory is described in terms of utilities (ordinal preference functions) and probabilities. Barring a few exceptions (e.g., Friedman and Savage, 1948, consider utility functions with both concave and convex segments), utility is typically considered concave over the entire domain.

Most of the literature on information security investments has taken an Expected Utility Theory approach to decision making under risk. Gordon and Loeb (2002) derive an economic model that determines the optimal amount to invest in information security for risk-neutral firms. They argue that the key in analyzing information security decisions is not the vulnerability (or the expected loss without investment in security), but the reduction in expected loss with the investment in security. Gordon and Loeb determine the optimal level of investment by maximizing the expected benefit of investment in security which is expressed in terms of the probability of a threat occurring, the probability of a realized threat being successful, and the loss of a realized threat. They conclude that the optimal investment for protecting a given information set has an inverted parabolic relationship with the information set's vulnerability. Huang, Hu and Behara (2005) demonstrate that similar results apply to risk-averse firms.

Gordon and Loeb, as well as Huang, Hu and Behara assume that decision makers behave in accord with EUT. However, there is ample evidence that decision-making under uncertainty often deviates from EUT predictions (Tversky and Kahnemann, 1974; Hogarth and Einhorn, 1990; Tversky and Koehler, 1994; Kuhn and Budescu, 1996; Fox and Tversky, 1998). Prospect Theory (Tversky and Kahnemann, 1974; Kahnemann and Tversky 1979; Tversky and Kahnemann, 1981) is a descriptive model that was developed to account for how people actually behave. According to this theory, people monitor gains or losses (deviations from the status quo or some other salient reference point), not final asset positions, while making decisions. The theory is described in terms of both a weighting function and a value function. The weighting function is non-linear, and it under-weights high probabilities and over-weights low probabilities. The value function is concave over gains, but convex and steeper over losses. Together, these functions lead to four different risk attitudes: risk seeking for gains of low probability, risk aversion for losses of low probability, risk aversion for gains of high probability, and risk seeking for losses of high probability. In other words, PT puts forth the argument that decision makers may be risk seeking under certain circumstances.

It is not clear whether PT or EUT applies to decisions involving optimal security investment. This is because investment in security is really about two kinds of losses – the expected loss from a security breach, and the cost of investment in security. Given that PT predicts risk seeking behavior for losses that occur with a high probability (plausible in today's security environment) firms may well be risk seeking in their behavior concerning investment in information security. However, there are several context-specific reasons why decision makers may behave in accord with EUT when considering investments in information security. First, absolute losses due to security breaches can far exceed those experimented with in PT, possibly instilling risk aversion even in the case of losses. Second, since decision makers involved in security investment decisions would be held personally responsible should there be a breach, they may exhibit more risk-averse behavior. Third, in choosing security investments, decision makers might properly ignore sunk cost effects because a minimum amount of security is mandated. Our study represents an initial attempt to determine whether PT or EUT more accurately models decision making behavior in the domain of information security investments.

3. RESEARCH METHOD

To study the applicability of PT in the context of optimal investment in information security, we modified the instrument used by Tversky and Kahnemann in their seminal papers (1974; 1979; 1981). Table 1 details the *hypotheses tested (in italics)*, the instrument, the **expected responses (in bold)**, and the ***observed responses (in bold italics)***.

Thirty four students enrolled in an information security course responded to our survey. The ordering of the questions in the instrument was randomized to remove any ordering effects. Data pertaining to 4 subjects were discarded due to incompleteness and suspicious responses (i.e., same choice was picked through the entire survey). We also collected demographic data such as age and gender, personal risk assessment, nature of job, and recent security breach history in the survey.

4. RESULTS AND DISCUSSION

In the third column of Table 1, the results in bold are supported (but not significant), those in bold and marked with an asterisk are significant, and the rest aren't supported. The test statistic used was the one-proportion, one-tailed z-test (H0: proportion of successes for population = 0.5; H1: proportion of successes for population > 0.5; $\alpha = 0.05$; $n = 30$).

Hypothesis 1 tests the basic premise of PT that people are risk averse with gains (1a) and risk seeking with losses (1b). While 1a was significantly supported, 1b was not supported. In fact, a majority of subjects made decisions opposite to that predicted by PT ($p < 0.05$). This may be because1b was not framed clearly enough as a choice between two losses. It is also likely that people react differently to losses when they are personally held responsible for the loss (as in the security investment case). It has also been suggested in the past literature (e.g., Harbaugh, Krause and Vesterlund, 2002) that while subjects' risk attitudes

are consistent with PT when pricing gambles, the theory is not robust when choosing between a gamble and its expected value.

Number	*[Hypotheses]*, Instrument, **Expected Responses**	***Observed Responses (n=30)***
1a	*[People overweight outcomes that are considered certain, relative to outcomes which are merely probable (certainty effect)]* Scenario: You estimate the expected loss that would result from a successful attack at $6 million. Given that estimate, which of the following two options would you choose? **a. Security package #1, which will reduce estimated losses by $2 million.** b. Security package #2, which provides a 1/3 probability of reducing estimated losses by $6 million and a 2/3 probability of not reducing estimated losses at all.	 ***0.83**** 0.17
1b	*[The preference between negative prospects is the mirror image of the preference between positive prospects (reflection effect)]* Scenario: You estimate the expected loss that would result from a successful attack at $6 million. Given that estimate, which of the following two options would you choose? a. Security package #1, which reduces estimated losses to $4 million. **b. Security package #2, which provides a 1/3 probability of reducing estimated losses to zero, and a 2/3 probability that estimated losses will be $6 million.**	 0.73 0.27
2a	*[Possibility versus probability of gains – high absolute value of outcome]* *[When gains are probable, people will choose the prospect that offers certain gains]* Scenario: Which security package will you choose? a. Security package #1, which provides a 45% chance of reducing expected losses by $60,000. **b. Security package #2, which provides a 90% chance of reducing expected losses by $30,000.**	 0.10 ***0.90****
2b	*[When gains are possible but not probable, people will choose the prospect that offers larger gain]* Scenario: Which security package will you choose? **a. Security package #1, which provides a 0.1% chance of reducing expected losses by $60,000.** b. Security package #2, which provides a 0.2% chance of reducing expected losses by $30,000.	 0.50 0.50
2c	*[Possibility versus probability of gains – low absolute value of outcome]* *[When gains are probable, people will choose the prospect that offers certain gains (certainty effect)]* Scenario: Which security package will you choose? a. Security package #1, which provides a 45% chance of reducing expected losses by $6000. **b. Security package #2, which provides a 90% chance of reducing expected losses by $3000.**	 0.07 ***0.93****
2d	*[When gains are possible but not probable, people will choose the prospect that offers larger gain]* Scenario: Which security package will you choose? **a. Security package #1, which provides a 0.1% chance of reducing expected losses by $6000.** b. Security package #2, which provides a 0.2% chance of reducing expected losses by $3000.	 ***0.53*** 0.47
3a	*[People's choices depend on framing of contingencies]* Scenario: Which of the following security packages will you choose?	

	a. Security package #1, which reduces expected losses by $30,000. b. Security package #2, which provides an 80% chance of reducing expected losses by $45,000.	***0.60*** 0.40
3b	*[In order to simplify the choice between alternatives, people often disregard components that the alternatives share, and focus on the components that distinguish them (isolation effect)]* Scenario: Attacks fail 75% of the time, and are successful 25% of the time. Two products have been identified that can be used if an attack is successful. Which of these would you choose? **a. Security package #1, which reduces expected losses by $30,000.** b. Security package #2, which provides an 80% chance of reducing expected losses by $45,000.	 ***0.60*** 0.40
3c	Scenario: Which of the following security packages will you choose? a. Security package #1, which provides a 25% chance of reducing expected losses by $30,000. **b. Security package #2, which provides a 20% chance of reducing expected losses by $45,000.**	 0.40 ***0.60***
4a	*People's choices depend on framing of outcomes:* *[People generally evaluate acts in terms of a minimal account, which includes only the direct consequences of the act]* Scenario: An anti-*virus* package you had purchased for $10,000 had failed to offer any protection against attacks. If you were now asked to purchase an anti-*worm* package for $10,000, will you purchase it? **yes** no	 0.40, 0.60
4b	*[A sunk cost effect arises when a decision is referred to an existing account in which the current balance is negative]* Scenario: An anti-*virus* package you had purchased for $10,000 had failed to offer any protection against attacks. If you were now asked to purchase another anti-*virus* package for $10,000, will you purchase it? yes **no**	 0.63, 0.37
5	*[Lower probabilities are over-weighted (insurance effect)]* Scenario: There is a 0.001 chance that you will incur a damage of $2 million if you do not invest in any security measures. Alternatively, you can invest $10,000 in a security package and avert all possibility of damage. Will you invest in the security package? **yes** no	 ***0.90****, 0.10

Table 1: *[Hypotheses]***,** Instrument**, Expected Responses,** and ***Observed Responses,***
***** significant at $p < 0.05$ (based on a one-proportion, one-tailed z-test)

Hypothesis 2 relates to how people react to prospects that are probable as against prospects that are merely possible. We tested this hypothesis for both low (2c and 2d) and high (2a and 2b) absolute outcomes. In the former case, when gains are probable (2c), we would expect people to be risk-averse with gains, as borne out by the significant support of this hypothesis. However, the non-linear weighting function over-weights low probabilities, thereby making the decision-maker more risk-seeking towards gains when gains are merely possible (2d). While this hypothesis shows the right direction, it is not significant. For the case of high absolute outcomes, we find that while 2a is significantly supported, results of 2b are inconclusive. This may be due to the fact that the value function is concave for gains, thereby reducing the effect of (over-weighted) very low probabilities for high absolute outcomes.

Hypothesis 3 tests how the framing of contingencies affects people's choices. This was done by breaking up Hypothesis 3 into 3 different questions. Question 3b is different from 3a in that it has an extra stage in the decision-making process. If the second stage is reached, then 3b reduces to 3a. Also note that 3b is identical to 3c in terms of probabilities and outcomes. However, as predicted by PT, a majority of people responded similarly to 3a and 3b, but differently to 3c. This is because, in order to simplify the choice between alternatives, people often disregard components that the alternatives share to focus more on the components that distinguish them. This hypothesis, while consistent with our results, was not significantly supported.

Hypothesis 4 tests how the framing of outcomes affects decision-makers' choices. We found no support for either minimal account, or sunk-cost effects. In fact, the responses in both cases seemed to favor the opposite of what we expected. This may be due to the context the questions were set in. For instance, in the case of 4b, the fact that the anti-virus package had failed, would actually encourage people to buy another anti-virus package since they still need to protect their systems from viruses. Similarly, in the case of 4a, the failure of an anti-virus package doesn't necessitate the need for an anti-worm package.

Hypothesis 5 tests how the insurance effect plays out in people's choices. We found significant support for the hypothesis. Subjects prefer a small loss over a small probability of a large loss. This occurs because very low probabilities are generally over-weighted.

5. CONCLUSION AND FUTURE WORK

The purpose of this research is to re-evaluate Prospect Theory and establish its relevance in the information security context. Preliminary results have shown partial support for the Prospect Theory hypotheses tested in this context. However, hypotheses 1b, 4a, and 4b were not supported, suggesting that in the context of investing in information security, decision makers sometimes behaved in accord with PT and other times in accord with EUT. Therefore, we plan to conduct further research to better understand the decision process underlying investments in information security.

REFERENCES

1. C.R. Fox and A. Tversky, "A Belief-Based Account of Decision Under Uncertainty", *Management Science*, vol. 44, no. 7, pp. 879-895, 1998.
2. M. Friedman and L. J. Savage, "The Utility Analysis of Choices Involving Risk", *Journal of Political Economy*, vol. 56, no. 4, pp. 279-304, 1948.
3. L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.
4. W.T. Harbaugh, K. Krause and L. Vesterlund, "Prospect theory in choice and pricing tasks," *Working Paper*, 2002.
5. R.M. Hogarth and H.J. Einhorn, "Venture Theory: A Model of Decision Weights", *Management Science*, vol. 36, no. 7, pp. 780-804, 1990.
6. C. D. Huang, Q. Hu, R. Behara, "In Search for Optimal Level of Information Security Investment in Risk-Averse Firms", *Third Annual Security Symposium*, ASU, Sept. 11-13, 2005.
7. D. Kahnemann and A. Tversky, "Prospect Theory: An Analysis of Decision under Risk", *Econometrica*, vol. 47, no. 2, pp. 263-292, 1979.
8. K.M. Kuhn and D.V. Budescu, "The Relative Importance of Probabilities, Outcomes, and Vagueness in Hazard Risk Decisions", *Organizational Behavior and Human Decision Processes*, vol. 68, no. 3, pp. 301-317, 1996.
9. A. Tversky and D. Kahnemann, "Judgment under Uncertainty: Heuristics and Biases", *Science*, vol. 185, no. 4157, pp. 1124-1131, 1974.
10. A. Tversky and D. Kahnemann, "The Framing of Decisions and the Psychology of Choice", *Science*, vol. 211, no. 4481, pp. 453-458, 1981.
11. A. Tversky and D. J. Koehler, "Support theory: a non-extensional representation of subjective probability", *Psychological Review*, vol. 101, pp.547-567, 1994.
12. J. Von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton Univ. Press, Princeton NJ, 1944.