Insider Behavior: An Analysis of Decision under Risk

Fariborz Farahmand and Eugene H. Spafford

Center for Education and Research in Information Assurance and Security
Purdue University, West Lafayette, Indiana, USA
{fariborz,spaf}@purdue.edu *

Abstract. There is considerable research being conducted on insider threats is directed to developing new technologies. At the same time, existing technology is not being fully utilized because of non-technological issues that pertain to economics and the human dimension. Issues related to how insiders actually behave are critical to ensuring that the best technologies are meeting their intended purpose. In our research, we have investigated accepted models of perceptions of risk and characteristics unique to insider threat, and we have introduced ordinal scales to these models to measure insider perceptions of risk. We have also investigated decision theories, leading to a conclusion that Prospect Theory, developed by Tversky and Kahneman, may be used to describe the risk-taking behavior of insiders and can be accommodated in our model. We discuss the results of validating that model with thirty-five senior information security executives from a variety of organizations. We also discuss how the model may be used to identify characteristics of insiders' perceptions of risk and benefit, their risk-taking behavior and how to frame insider decisions.

1 Who is an Insider?

A survey of the literature identifies several attempts to understand the insider threat and the behavior of insiders in organizations (e.g., [1]; [2]), and to provide technical defense against those threats (e.g., [3]; [4]). Bishop and Gates [5] explain that defining 'insider' as a binary condition is not appropriate and they instead define insiders based on their access attributes. However, currently there is no generally-accepted definition of an insider.

From an organizational perspective, is employment the defining factor? For example, are hours worked per week, or the person's history with that organization the defining aspects? Organizational behavioral studies do not support a mapping between these factors and the extent to which an individual employee perceives self as an insider within a particular organization (e.g., [6]). The main goals of our ongoing research on insider threats are to understand insider risk

* D. Chadwick, I. You and H. Chang (Eds.): Proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST2009), Purdue University, West Lafayette, USA, June 16, 2009. *Copyright is held by the author(s)*

taking behavior and to frame insider decisions on taking actions such as theft of information, sabotage, and fraud in organizations.

2 Insider Perception of Information Security Risks

Fischhoff et al. [7] investigated perceptions of risk, and particularly ways to determine when a product is acceptably safe. Their model can be adopted and used to define insider risk associated with misbehavior:

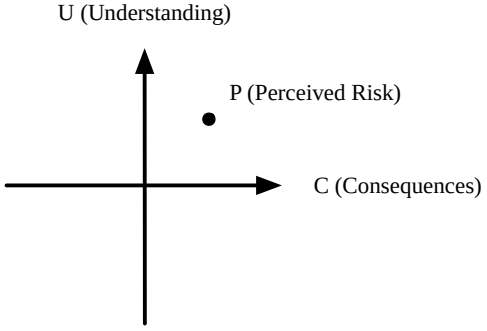
1. Does the insider voluntarily get involved in the risk situation (voluntariness)?
2. To what extent is the risk of consequence from the insider's action to him/her immediate (immediacy of effect)?
3. To what extent are the risks known (precisely) by the insider who is exposed to those risks (knowledge about risk)?
4. To what extent are the risks precisely known and quantified (knowledge to science)?
5. To what extent can the insider, by personal skill or diligence, avoid the consequences to him/her while engaging in the untoward activity (control over risk)?
6. Does the risk affect the insider over time or is it a risk that affects a larger number of people at once (chronic-catastrophic)?
7. Are these risks new to the insider or is there some prior experience/conditioning (newness)?
8. Is this a risk that the insider has rationalized and can think about reasonably calmly (common-dread)?
9. When the risk from the activity is realized in the form of consequences to the insider (severity of consequences)?

It has been shown that unknown risk and dread risk can be used to account for about 80 percent of the results generated by using all nine variables that were originally introduced by Fischhoff and his colleagues (e.g., [8]). (We note that the nine risk factors given above may not apply in extreme cases involving drugs or ideology.)

We formulated a model based on the psychometric model of risk perception developed by Fischhoff, Slovic and others, in which characteristics of a risk are correlated with its acceptance. We then modified that model to accommodate factors present in insider misuse and to condense Fischhoff's nine variables of risk – listed above – by considering understanding (familiarity and experience) and consequences (scope, duration, and impact) to the insider as the two principal characteristics of information security and privacy risks.

If we explore the fear insiders have of the potential effects to them of the risks of perpetrating IT misuse, we can model the consequences of the breach to the insider. To model this, we consider three main questions: 1) How serious are effects perceived by insiders? 2) How immediate are effects on insiders, and 3) How much do insiders fear the effects? Analyzing these questions enables us to assign a simple metric to this dimension of the model. We define five levels of consequence:

Fig. 1. Characteristics of Perceptions of Information Security Risks



1. Level 1: Effects are trivial, temporary and commonplace
2. Level 2: Effects are potentiality serious but treatable/recoverable
3. Level 3: Effects are serious, long term but considered normal
4. Level 4: Effects are serious, ongoing and raise deep concerns
5. Level 5: Effects are catastrophic, ongoing and highly feared

The level definitions ('trivial,' 'serious,' etc.) are based on those published by the National Institute of Standards and Technology (see [9]). Level 5 and level 1 represent the highest and lowest level of consequences to insiders, respectively.

For the second dimension, understanding, we can explore the factors motivating users to consider certain risks while dismissing others. These questions are intended to identify affective factors that influence users' cognitive understanding of cause and effect. This resolves into two main questions: 1) who (among the insider group) understand the hazard? 2) What do insiders know?

Our framework for categorizing understanding is based on the work of Bloom and Krathwhol [10]. In this, our interest is in understanding risk causes and effects using the cognitive domain, and what adds to insiders' motivation to increase understanding using the affective domain. We obtain the following six-level metric for the understanding dimension of our model by answering these questions:

1. Level 1: Evaluation: Can the insider make judgments about the value of ideas or materials?
2. Level 2: Synthesis: Can the insider build a structure or pattern from diverse elements?
3. Level 3: Analysis: How insiders distinguish between facts and inferences.
4. Level 4: Application: How insiders use a concept in a new situation or unprompted use of an abstraction.
5. Level 5: Comprehension: Can the insider understand the problem, for e.g. state a problem in his/her own words?
6. Level 6: Knowledge: Can the insider recall data or information?

Level 6 and level 1 represent the lowest and the highest level of understanding, respectively.

The perceived risk in our model is a function of consequence and understanding. An approximate perceived risk score may be constructed from the consequence metric and the inverse of the understanding metric. The perceived risk score therefore increases whenever the consequences are more severe for insiders, and decreases as the insider gains deeper understanding of the nature and limits of the risk. Some cases may not match this model exactly but this score is nonetheless a good match for many case studies and the experiences of the experts interviewed in our validation study.

If managers understand the dynamic processes by which insiders learn about risk, they can then use that knowledge to choose among alternatives that have different uncertainties, risks and benefits. Our research addresses the dynamics of perception by including a variable time element in our model that causes the risk score to decay with time. That extension will not be discussed here (for full details of this model see [11]) but may be employed as part of a more extensive evaluation of risk perception.

3 Model Validation

To validate our model, we presented it to thirty-five senior information security executives in industry and governmental organizations across the U.S. Following a ten-minute description of our model, we conducted our studies in structured one-on-one meetings and telephone interviews.

During the meetings/interviews we asked these executives if they were able to map the perceived risk of the worst information security incident that they had experienced into our model. We also asked questions such as: Were those incidents caused by insiders or outsiders? How do you describe the level of the consequences and understanding of risks of those incidents? Do you believe this level was the same for all the stakeholders?

These executives each had at least a decade of experience with a large range of information security issues. All these executives were able to map their perceived risk into our model. They were also able to estimate the range of perceived risk by different stakeholders. However, the interviewees stated that perceived risk is not the only factor that we should investigate in modeling insider risk and framing insider decisions, and the perceived benefit is likely to play a more important role in insider decisions.

4 Fraud Triangle

Most of the law enforcement agents who were interviewed in our research indicated the Fraud Triangle was a model that they regularly used when investigating insider crime. Joseph T. Wells [12], a retired law enforcement agent, developed this model as a model of elements supporting and motivating fraud. Mr. Wells's model was influenced by the research of Donald R. Cressey (1919 – 1987), a

sociologist known for his work in organized crime investigation. Motive, opportunity, and rationalization are the three elements of Wells's model, also known as the Fraud Triangle.

Combining our model for risk perception with Wells's model indicates that management should ensure that discovered misuse is punished appropriately, and that appropriate audit controls are in place. The combination further suggests that opportunity may be countered by random observation and unpublicized controls, thus introducing additional uncertainty to the perception of risk.

5 Inverse Relationship between Perceived Risk and Benefit

Similar to the arguments made by decision scientists about the role of affect in human decision making (e.g., [13]), we argue that insiders use an affect heuristic to make judgments. That is, representations of events in insiders' minds are tagged to varying degrees with affect. Insiders consult or refer to an affective pool in the process of making judgments. Using an overall and affective impression can be far easier than weighing the pros and cons or retrieving from memory many relevant examples, especially when the required judgment is complex and includes many unknown variables.

The affect heuristic also predicts that using time pressure to reduce the opportunity for analytic deliberation should enhance the inverse relationship between perceived benefits and risks—the higher the perceived benefit, the lower the perceived risk, and vice versa. Finucane et al. [13] showed that the inverse relationship between perceived risks and benefits increased greatly under time pressure as predicted. This is consistent with Zajonc's findings [14] that affect influences judgment directly and is not simply a response to a prior analytic evaluation.

Kahneman and Lovallo [15] explain the concept of inside view–a forecast is generated by focusing on the case at hand, for e.g., by considering the plan and the obstacles to its completion, and outside view–a focus on the statistics of a class of cases similar in respects to the present one. Our findings indicate that insiders are normally biased in favor of the inside view and tend to neglect the statistics of the past. This characteristic makes them capable of two biases–also known as isolation errors ([15]): Their forecasts of future outcome are often anchored on plans and scenarios of success rather than on past results, and are therefore optimistic; their evaluations of single risky prospects neglect the possibilities of pooling risks.

Another explanation for the inverse relationship between perceived risk and benefit by insiders could be that perceived benefits–compared to perceived risks–are simply more evaluable, largely they are conceptualized unidimensionally, and are psychologically represented in terms of a convenient and numerical scale ([16]). Lichtenstein and Slovic [17] also explain that the amount to win can directly translate to an amount to bid–in an insider's case to take different approaches to commit the crime, or to commit or not to commit the crime at

all. Probabilities of winning and losing, presented in probability units, are more difficult to translate into monetary units. This can lead insiders to decisions that are highly correlated with the amount to win but poorly reflect the variations in probabilities and amount to lose.

6 Framing Insider's Decisions

Classical decision theory ([18], [19]) frame the choice people make in terms of four basic elements:

1. A Set of potential actions (A_i) to choose between,
2. A set of events or world states (E_j),
3. A set of consequences obtained (C_{ij}) for each combination of action and event, and
4. A set of probabilities (P_{ij}) for each combination of action and event

According to classical decision theory, the expected value of an action is calculated by weighting its consequences over all events by the probability the event will occur. Classical decision theories neither adequately explain the insider behavior nor do they assist managers in selecting appropriate control measure(s) to prevent/minimize damage or loss caused by insider misuse. For example, a manger might be deciding whether to install misuse detection software in his company's network. Installing or not installing software responds to two actions A_1 and A_2. The expected consequences of either action depend upon whether misuse occurs. Misuse occurring or not occurring corresponds to two events E_1 and E_2. Installing misuse detection software may reduce the consequences (C_{11}) of misuse occurring. As the probability of misuse occurrence increases, use of software seems to be more attractive.

From probability theory, it can be shown that the return to a manager is maximized by selecting the alternative with the greatest expected value. The expected value of an action A_i is calculated by weighting its consequences C_{ik} over all events k, by the probability P_{ik} the event will occur. The expected value of a given action A_i is therefore:

$$EV[A_i] = \sum_k P_{ik} C_{ik} \tag{1}$$

More generally, a manager's preference for a given consequence C_{ik} might be defined by a value function $V(C_{ik})$, which transforms consequences into preference values. The preference values are then weighed using the same equation. The expected value of a given action A_i becomes:

$$EV[A_i] = \sum_k P_{ik} V(C_{ik}) \tag{2}$$

Expected utility theory extended expected value theory to describe how people make certain economic choices ([18]). Subjective utility theory added the

notion that uncertainty about outcomes could be represented with subjective probabilities ([19]) and multi-attribute utility theory ([20]) extended subjective utility theory to the case where the decision maker has multiple objectives.

Traditional methods of engineering risk analysis and expected utility decisions, despite all their differences, share a common core: Both rely on the assumption of complete rationality. However, the results of studies by decision science researchers in the past four decades contrast with the outcomes of these traditional methods, which stem from the work of Daniel Bernoulli and Thomas Bayes in the seventeenth century. Not all decisions are completely rational.

A large literature has been developed showing that the framing of decisions can have practical effects for both individual decision makers ([21], [22]) and group decisions ([23]). A number of approaches have been developed for mathematically describing human judgments. These approaches include the use of policy-capturing models in social judgment theory, probabilistic mental models, multiple-cue probability learning models, and information theory. Some researchers use a cognitive continuum theory that builds upon social judgment by distinguishing judgments on a cognitive continuum varying from highly intuitive decisions to highly analytical decisions (e.g., [24]).

Tversky and Kahneman [25] made a key contribution to the field when they showed that many of the previously-mentioned discrepancies between human estimates of probability and Bayes' rule could be explained by the use of three heuristics:

Representativeness. In the representativeness heuristic, the probability that, for example Bob is a criminal insider is assessed by the degree to which he is representative of, or similar to, the stereotype of criminal insiders. This approach for estimating probability can lead to serious errors because similarity, or representativeness, is not influenced by several factors that should affect determination of probability.

Availability. There are situations in which an information security executive conceptualizes the frequency of a class or the probability of an event by the ease with which past instances or occurrences can be brought to mind. For example, an information security executive may assess the risk of disclosure of information among financial institutions by hearing about such occurrences from one's acquaintances. Availability is a useful clue for assessing frequency or probability, because instances of large classes are usually recalled better and faster than instances of less frequent classes. However, availability is affected by factors other than frequency or probability, e.g., systematic non-reporting or underreporting of system penetrations within an industry. Consequently, the reliance on availability can lead to biases.

Adjustment and anchoring. In many situations, information security executives make estimates by starting from an initial value that is adjusted to yield the final answer. The initial value, or starting point, may be suggested by the formulation of the problem, or it may be the result of a partial computation. In either case, adjustments are typically insufficient. That is, different starting points yield different estimates, which are biased toward the initial values.

The notion of heuristics and biases has had a particularly formative influence on decision theory. A substantial body of work with applications in medical judgment and decision making, affirmative action, education, personality assessment, legal decision making, mediation, and policy making has emerged that focuses on applying research on heuristics and biases ([26]).

7 Prospect Theory

Among the different decision theories that we investigated, Prospect Theory by Amos Tversky and Daniel Kahneman (who won the 2002 Nobel Prize in Economics for its development) – best describes the behavior of insiders.

Prospect Theory distinguishes two phases in choice processes: framing and valuation ([27]). In the framing phase, the insider constructs a representation of acts, contingencies, and outcomes that are relevant to the decision. In the valuation phase, the insider assesses the value of each prospect and chooses accordingly.

From the cases that we discussed with our interviewees we found that decision theories based on the expected utility theory–where risk aversion and risk seeking are determined solely by the utility function–do not adequately explain the risk taking behavior of insiders. Insiders normally make decisions based on change of wealth rather than total gain–a behavior that is well explained by Prospect Theory. This also correlates with our model, in that insiders may not fully understand the risks of a crime that might be immensely favorable if successful.

This finding is also consistent with the results of some previous studies. For example Wood [28] finds insiders to be risk averse and their ultimate fear is to be discovered before they have mounted a successful attack. Risk aversion is the reluctance of an insider to accept a bargain with an uncertain payoff rather than another bargain with more certain, but possibly lower expected payoff. Expected value maximization is problematic in framing an insider's decision because it does not allow decision makers to exhibit risk aversion.

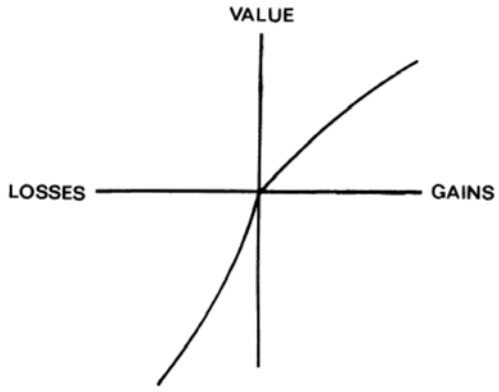
Prospect Theory has been successful in explaining individual differences that have been observed in the laboratory and outside the laboratory studies ([29]; [30]; [31]). However, some studies do not completely support applications of Prospect Theory in the real world ([32]; [33]).

Following Kahneman and Tversky, we can parameterize the value function in Prospect Theory as a power function (see Figure 2):

$$V(x) = \begin{cases} x^{\alpha} & x \geq 0 \\ -\lambda(-x)^{\beta} & x < 0 \end{cases}$$

Where $\alpha, \beta > 0$ measure the curvature of the value function for gains and losses, respectively, and k is the coefficient of loss aversion. Thus, the value function for gains (losses) is increasingly concave (convex) for smaller values of $\alpha(\beta) < 1$, and loss aversion is more pronounced for larger values of $\lambda > 1$. Tversky and Kahneman estimated median values of $\alpha = \beta = .88$, and $\lambda = 2.25$

Fig. 2. Value function from Prospect Theory (adopted from [27])



among their sample of college students. The degree of curvature of the value function represents the insider's sensitivity to increasing units gained or lost.

Expected utility theory and most normative models of decision making under risk assume the principle of description invariance: Preferences among prospects should not be affected by how they are described. Decision makers act as if they are assessing the impact of options on final assets ([31]). Prospect Theory acknowledges that choices are influenced by how prospects are cognitively represented in terms of losses versus gains and their associated probabilities–this characteristic of Prospect Theory explains the influence of perceptions on insider decisions.

We argue that the significant ability of Prospect Theory in framing and editing operations, compared to other decision theories, best describes the behavior of insiders.

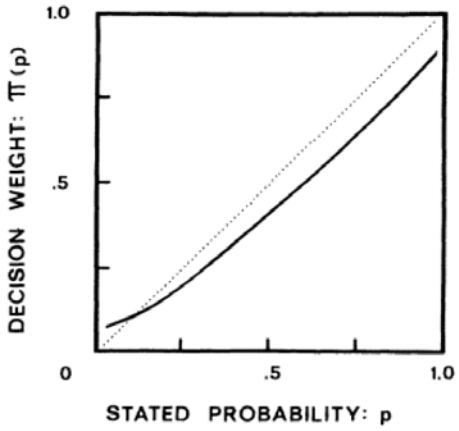
The Weighting function in Prospect Theory can be shown as follow:

$$w(p) = \frac{\delta p^{\gamma}}{\delta p^{\gamma} + (1-p)^{\gamma}}$$

Where $\delta > 0$ measures the elevation of the weighting function and $\gamma > 0$ measures its degree of curvature. Figure 3 represents shape of this weighting function:

The inverse-S-shaped weighting function is characterized by a tendency to overweight low probabilities and underweight moderate to high probabilities. Although the shape of the value function implies risk aversion for gains and risk seeking for losses, this pattern seems to be reversed for low-probability events and reinforced for high-probability events.

Fig. 3. Weighing function from Prospect Theory (adopted from [27])



8 Summary and Conclusion

This paper describes on the role of perceptions of risk and benefit of insiders in taking actions such as theft of information, sabotage, and fraud in organizations. We use the theoretical foundation of perception of risk built by Baruch Fischhoff, Paul Slovic, and of behavioral economics by Daniel Kahneman and Amos Tversky. We identify consequences and understanding as two main characteristics of perceived risk by insiders. We contend that perceived benefit plays an important role in insider decisions and that classical decision theories cannot adequately explain insider behavior.

Making effective decisions to confront insider threats requires understanding insiders' risk taking behavior and their decision heuristic. We believe that there is significant value to including risk perception management as part of a comprehensive security plan. Technical controls continue to be important, especially when coping with outsider attacks and unexpected failures. However, not all security problems can be addressed with IT-based defenses. Our research results provide one more approach to defending important computing assets against insider misuse.

9 Acknowledgments

This material is based in part upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of

Homeland Security, the I3P, or Dartmouth College. Sponsors of the Center Education and Research in Information Assurance and Security (CERIAS) also supported portions of this work. The authors would also like to acknowledge the contribution of Mr. William Keck in literature review.

References

1. Brackney, R.C., Anderson, R.H.: Understanding the insider threat. Proceedings of a March 2004 Workshop, RAND Corporation (2004)
2. Greitzer, F.e.a.: Combating the insider cyber threat. IEEE Security and Privacy, pp. 61-64. (2008)
3. Maloof, M., Stephens, G.: Elicit: A system for detecting insiders who violate need-to-know. Lecture Notes in Computer Science, 4637, pp.146-166 (2007)
4. Stolfo, S., Bellovin, S., Hershkop, S., Keromytis, A., Sinclair, S., Smith, S.: Insider attack and cyber security. Advances in Information Security, Springer (2008)
5. Bishop, M., Gates, C.: Defining the insider threat. Proceedings of the Cyber Security and Information Intelligence Research Workshop, article 15 (2008)
6. Stamper, C.L., Masteson, S.: Insider or outsider? how employee perception of insider status affect their work behavior. Journal of Organizational Behavior, 23, pp. 875-894 (2002)
7. Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B.: How safe is safe enough? a psychome-tric study of attitudes towards technological risks and benefits? Policy Sciences, 9(2), pp. 127-152 (1978)
8. Slovic, P.: Perceptions of risk. Science, 236, pp.280-285 (1987)
9. Stoneburner, G., Gougen, A., Feringa, A.: Risk Management Guide for Information Technology Systems. NIST SP800-30 (2002)
10. Bloom, B.S., Krathwohl, D.R.: Taxonomy of educational objectives: The classification of educational goals, by a committee of college and university examiners. Handbook 1: Cognitive domain, New York, Longmans (1956)
11. Farahmand, F., Atallah, M., , Kensynski, B.: Incentives and perceptions of information security risks. Proc. of the Twenty Ninth International Conference on Information Systems, Paris (2008)
12. Wells, J.T.: Principles of Fraud Examination. John Wiley & Sons (2005)
13. Finucane, M.L., Alhakami, A., Slovic, P., Johnson, S.M.: The affect heuristic in judgments of risks and benefits. Journal of Behavioral Decision Making, Vol. 13, pp. 1-17 (2000)
14. Zajonc, R.B.: Feeling and thinking: Preferences need no inferences. American Psychologist, Vol. 35, pp.151-175 (1980)
15. Kahneman, D., Lovallo, D.: Timid choices and bold forecasts: A cognitive perspective on risk taking. Management Science, Vol. 39, No. 1, pp. 17-31 (1993)
16. MacGregor, D.G.e.a.: Perception of financial risk: A survey study of advisors and planners. Journal of Financial Planning, Vol. 12 Issue 8, pp. 68-86 (1999)
17. Lichtenstein, S., Slovic, P.: Reversals of preference between bids and choices in gamble decisions. Journal of Experimental Psychology, Vol. 89, No. 1, pp. 46-55 (1971)
18. von Neumann, J., Morgenstern, O.: Theory of Games and Economic Behavior. Princeton University Press (1947)
19. Savage, L.J.: The Foundations of Statistics. John Wiley & Sons (1954)

20. Kenney, R.L., Raiffa, H.: Decisions with Multiple Objectives: Preferences and Value Tradeoffs. John Wiley & Sons (1976)
21. Kahneman, D., Slovic, P., Tversky, A.: Judgment under uncertainty; heuristics and biases (1982)
22. Heath, L., Tindale, R., Edwards, J., Posavac, E., Bryant, F., Henderson-King, E., Suarez-Balcazar, Y., Myers, J.: Applications of Heuristics and Biases to Social Issues. Plenum Press (1994)
23. Paese, P.W., Bieser, M., Tubbs, M.E.: Framing effects and choose shifts in group decision making. Organizational Behavior and Human Decision Processes, 56, pp. 149-165 (1993)
24. Hammond, K.R.: Naturalistic decision making from a brunswikian viewpoint: Its past, present, future. In G. A. Klein, J., Orasanu, R., Calanrewood, Zsambok, E., (Eds.) Decision making in action: Models and Methods (pp. 205-227). Norwood, Albex (1993)
25. Tversky, A., Kahneman, D.: Judgment under uncertainty: Heuristics and biases. Science, 185, pp. 1124-1131 (1974)
26. Lehto, M.R., Buck, J.R.: Introduction to Human factors and Ergonomics for Engineers. CRC Press (2008)
27. Tversky, A., Kahneman, D.: Prospect theory: An analysis of decisions under risk. Econometrica, Vol. 47, No 2, pp. 263-291 (1979)
28. Wood, B.: An insider threat model for adversary simulation. SRI International, Research on Mitigating the Insider Threat to Information Systems - #2 Proceedings of a Workshop Held by RAND (2000)
29. Camerer, C.F.: Prospect theory in the wild. Cambridge Univ. Press, Cambridge, UK, (2000)
30. Odean, T.: Are investors reluctant to realize their losses? Journal of Finance, 53, pp. 1775-1798 (1998)
31. Trepel, C., Fox, C.R., Poldrack, R.A.: Prospect theory on the brain? toward a cognitive neuroscience of decision under risk. Cognitive Brain Research, Vol. 23, No 1, pp. 34-50 (2005)
32. Levy, M., Levy, H.: Prospect theory: Much ado about nothing. Management Science, Vol. 48, No. 10, October 2002, pp. 1334-1349 (2002)
33. Schroeder, N.J.: Using prospect theory to investigate decision-making bias within an information security context. Dept. of the Air Force Air University, Air Force Institute of Technology (2005)