Communications of the Association for Information Systems

Volume 35 Article 7

9-2014

Framing Information Security Budget Requests to Influence Investment Decisions

Nicole L. Beebe
University of Texas at San Antonio, nicole.beebe@utsa.edu

Diana K. Young
University of Texas at San Antonio

Frederick R. Chang
21CT, Inc.

Recommended Citation

Beebe, Nicole L.; Young, Diana K.; and Chang, Frederick R. (2014) "Framing Information Security Budget Requests to Influence Investment Decisions," *Communications of the Association for Information Systems*: Vol. 35 , Article 7.
DOI: 10.17705/1CAIS.03507
Available at: https://aisel.aisnet.org/cais/vol35/iss1/7

Communications of the Association for Information Systems

CAIS

Framing Information Security Budget Requests to Influence Investment Decisions

Nicole L. Beebe

University of Texas at San Antonio

Nicole.beebe@utsa.edu

Diana K. Young

University of Texas at San Antonio

Frederick R. Chang

21CT, Inc.

Abstract:

Researchers studying the economics of information security have traditionally focused on the use of rational choice decision models for evaluating investment alternatives. Security investment decisions involve risk, and several researchers have noted that risk-related decisions often violate the fundamental principles of rational choice decision models. This study tests the prevailing presumption in published research that information security investment decisions are made in an entirely rational manner. We empirically validated our hypothesis that information security investment decision makers in fact exhibit preference reversals when faced with competing budget alternatives involving risk. Specifically, we observed the framing effect under prospect theory, which suggests that individuals exhibit unique risk attitudes when evaluating gain-related and loss-related risk decisions. Accordingly, we argue that existing, widely accepted rational choice and economic models for information security investments need to be supplemented with risk perception measurement and account for individual level decision biases.

Keywords: Information Security, Security Economics, Security Management, Prospect Theory, Decision Theory.

Volume 35, Article 7, pp. 133-143, September 2014

The manuscript was received 26/07/2013 and was with the authors 5 months for 3 revisions.

I. INTRODUCTION

The pursuit of information security is concerned with protecting the confidentiality, integrity, and availability of information systems against adverse events and exploitation of system vulnerabilities. To achieve this goal, organizations implement controls. Controls include technologies, human resources, processes, training, and other initiatives. Recent research indicates that implemented controls may be reducing the effectiveness of certain security exploits (Richardson, 2011). Fewer organizations are reporting incidents of device theft, insider abuse, denial of service, financial fraud, password sniffing, and wireless network exploits. However, incidents involving botnets, malware infections, and phishing are increasing, which indicates that organizations need to implement additional controls and/or improve their existing controls to thwart these and other newly identified security threats.

Efforts aimed at improving an organization’s security generally require money to fund the development of necessary controls. However, Richardson (2011) found that a third of the 351 security practitioners surveyed by the Computer Security Institute (CSI) felt that the organization they worked for underfunded information security efforts. Individuals included in this sample represented a wide range of industry sectors, organizational sizes, and job titles. Furthermore, other research indicates that both information technology (IT) and information security budgets have declined in recent years (Stöwer & Kraft, 2012). Accordingly, two key challenges facing information security professionals are: 1) determining how much they should spend on security initiatives, and 2) convincing upper management to fund the necessary initiatives.

Rational choice and economic models have been developed to help decision makers determine the optimal amount they should spend to protect information assets (Bodin, Gordon, & Loeb, 2005; Cavusoglu, Cavusoglu, & Raghunathan, 2004a; Cavusoglu, Mishra, & Raghunathan, 2004b; Cavusoglu, Raghunathan, & Yue, 2008; Gordon & Loeb, 2002; Herath & Herath, 2008; Wang, Chaudhury, & Rao, 2008). These models focus on calculating the expected utility of a security initiative by comparing the resulting quantitative benefits to the costs of implementing and maintaining the security controls. However, security benefits are difficult to quantify because the benefit is a function of loss avoidance. Accordingly, benefit quantification inherently depends on an accurate and reliable method to determine the probability of a loss occurring, but actuarial data to support such a process is lacking. Many senior managers are cognizant of this difficulty, which then informs their perceptions of information security budget justifications and subsequent budget decisions. Accordingly, some practitioners use a modified approach that examines costs and benefits but places less emphasis on the formal quantification of benefits (Gordon & Loeb, 2006). In addition, some information security practitioners rely on past years’ budgets. Reliance on past years’ budgets is commonly criticized in the industry because, while expedient, it is important to fully consider and incorporate the upcoming year’s business goals, which may vary from the previous year’s goals. Many contend that the budgeting process should be an ongoing process throughout the year rather than an annual event because, otherwise, the budget fails to evolve. That concern is compounded when the budget is substantially derived from the previous year’s budget.

Once an investment request has been developed, information security professionals face the additional challenge of convincing higher-level managers that the initiative is necessary and should be funded. Top-level management consider information security investment requests amid competing funding requests across their organizations and they often have to make trade-off decisions amidst limited budgets. Accordingly, many factors, including qualitative considerations, impact managers’ investment decisions (Gordon, 1989). Whether the factors are qualitative or quantitative, information security investment research to date contends and assumes that the eventual investment decisions are rational.

However, long-standing behavioral and decision making research contends that individuals exhibit preference reversals that violate the axioms of rational choice models when making decisions that are characterized by risk (the potential for loss) and uncertainty (the probability of an outcome is unknown) (Kahneman & Tversky, 1979; Slovic, Fischhoff, & Lichtenstein, 1977). To explain these pervasive inconsistencies, Kahneman and Tversky (1979) have proposed prospect theory, which they characterize as an approximate description of the processes individuals use to evaluate risky prospects. The theory contends that individuals evaluate risk-related options using a two-step process. In the first step, individuals apply heuristics to simplify their understanding of their alternative choices. While these simplifying rules work well in some contexts, they can lead to deviations from rational choice models when evaluating risky prospects. In the second step, individuals evaluate the expected utility of each prospect and select the option that they perceive to provide the greatest utility. During this evaluation process, prospect theory contends that individuals apply an asymmetric S-shaped value function (Figure 1). For each prospect, the value function is multiplied by the outcome's probability of occurrence and its value. As the slope of this value function is more extreme for losses, individuals perceive the derived negative utility of a loss to be more extreme than the derived positive utility resulting from a gain of the same relative size.

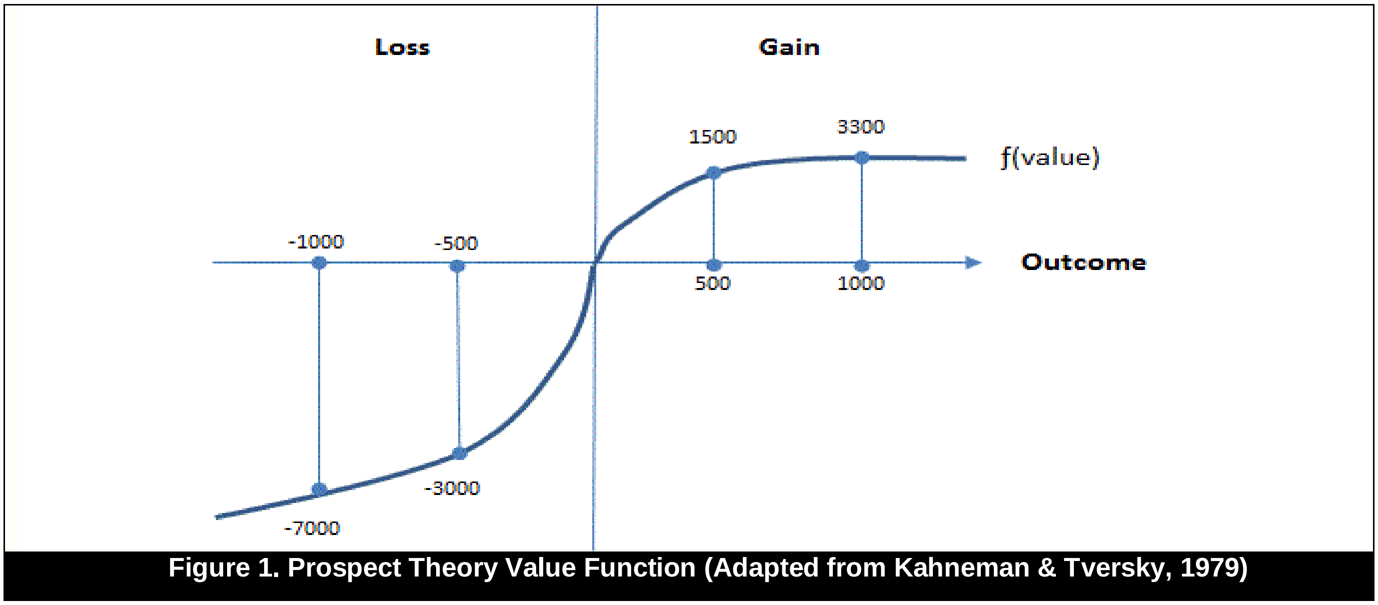

Figure 1. Prospect Theory Value Function (Adapted from Kahneman & Tversky, 1979)

Central to prospect theory is the concept of framing, which is the manner in which a statement or question is worded, such that the wording influences the "decision maker's conception of the acts, contingencies, and outcomes" of the given options (Tversky & Kahneman, 1981, p. 453). Many studies, by Tversky, Kahneman and others, have replicated Tversky and Kahneman's work and have shown that individuals largely prefer risk-averse options when evaluating gains and risk-seeking options when evaluating losses. Prospect theory is considered the most influential of all descriptive decision theories (Crozier & Ranyard, 1997) and has been used to study risk-related decisions in a variety of disciplines (Church, Libby, & Ping, 2008; Devers, McNamara, Wiseman, & Arrfelt, 2008; Edwards, Miles, & von Winterfeld, 2007; Latham & Braun, 2009; Wagner, Hennig-Thurau, & Rudolph, 2009). For example, Church et al. (2008) found that, when evaluating incentive-based contracts, individuals strongly preferred bonus-framed versus penalty-framed contracts. Similarly, Wagner et al. (2009) found that demotions from hierarchical loyalty program had a stronger negative impact on customers' loyalty intentions than did promotions to such programs of an equivalent size.

There is little certainty in information security. Some say the only certainty is "when, not if"—that is, that all organizations will be compromised at some point. That certainty gives way to new uncertainties, however, regarding the tangible and intangible impact of a potential compromise. Accordingly, information security investment decisions involve risk. Over-investment risks dollars that could be spent operationally on other projects. Under-investment risks information security, productivity, and stakeholder confidence in the organization.

Certainly, the organizational decision making process pertaining to resource investment is complex and typically transcends the singular individual. We do not contend the information security investment decision is an individual-level decision in most cases. However, since individual decision makers are significant input variables and indeed influence the organizational decision, individual-level decision making biases are important to consider.

Past normative decision making models for information security may be improved by accounting for the impact of individual risk perceptions and biases on otherwise rational decisions. This research empirically investigated whether individual information security investment decision makers exhibit risk preference reversals when evaluating budget alternatives involving risk. This is important since prevailing economic decision making models for information security do not account for, nor acknowledge, the potential for preference reversals. The ability to model decision biases and moderate their effect in a decision making model is important when the inputs to the model are subjective in nature. Many of the existing information security prescriptive models require subjective estimating critical input parameters because quantified values that are known to be reliable and valid simply do not exist. For example, some models require estimating the percentage of dishonest users in the organization, the value received by a hacker from breaking into a system, or the penalty for an intrusion.

Specifically, we test the framing effect under prospect theory, which suggests that individuals exhibit unique risk attitudes when evaluating gain-related and loss-related risk decisions (Kahneman & Tversky, 1979). We focus on framing effects for two reasons: 1) to demonstrate that information security professionals do deviate from rational choice models when evaluating security related investment decisions, and 2) to show that investment requestors can influence decision makers' behavior by simply changing the wording of their requests.

Prospect theory research has shown many times and many contexts that, when faced with risk-related decisions that are framed as gains, individuals usually prefer more risk-averse options. In contrast, individuals usually prefer riskier options when decision choices are framed as losses. Yet, the absence of individual decision bias variables in extant information security investment models suggests the field may view the decision as entirely rational. Further, while the information security investment decision is often an organizational-level decision in larger organizations, it is still heavily influenced by individual decision making biases of individual contributors.

Based on this and the fact that top managers consider both qualitative and quantitative factors when making investment decisions (Gordon, 1989), we contend that the framing of information security investment requests influences the investment decisions made by top management. For information security personnel, the implication is that the age-old "fear, uncertainty, and doubt (FUD)" strategy of scaring top management into investing in information security may actually have the **opposite** effect than was intended. Nonetheless, organizations still frequently evaluate investment options relative to vulnerabilities and the likelihood that the vulnerabilities will be exploited (Buck, Das, & Hanf, 2008; Stöwer & Kraft, 2012)—the negative impact of not investing, rather than the positive impact of investing. When proposing security investment options, information security personnel have the option to discuss the impact of the investment (or lack thereof) in terms of the assets that will be protected, or in terms of the assets that will be lost. For researchers, this may explain some of the error involved with purely rational-choice and/or economic models. For top management, the implication is that decisions and support systems may be improved when the possibility of preference reversal is realized and accounted for.

According to rational choice economic models, investment framing should have no impact on decision makers' preferences among investment options. However, prospect theory research has shown that framing does influence risk-related decisions. To address this issue, we conducted a scenario-based empirical study of the information security investment decisions made by information security managers and executives.

II. BIASES IN DECISION MAKING

Past research indicates that high-stakes decisions involving uncertainty "fall prey to a wide range of potentially harmful biases" (Kunreuther et al., 2002, p. 259) that result from heuristics that are applied during the editing and evaluation phases of the decision making process. Specifically, Bazerman (2006) notes that the availability, representativeness, and affect heuristics can significantly bias perceptions regarding decision options.

The availability heuristic refers to a mental shortcut individuals use to assess the frequency of an event based on how readily information regarding similar event instances can be retrieved from memory. While this unconscious process allows individuals to quickly assess event likelihood, it can also result in biased decision processes when evaluating events where risk is involved. For example, Bazerman (2006) notes that applying the availability heuristic can result in frequency over-estimation of extremely vivid and/or very recent events, frequency under-estimation of events that are difficult to recall or understand, and over-estimation of event correspondence when the decision maker has past experience involving event co-occurrence. In terms of information security investment decisions, applying this heuristic can result in decision makers greatly underestimating the probability of security events resulting from newly identified or unusual threats, while overestimating the probability of widely discussed, highly destructive events.

The representative heuristic refers to the unconscious process of comparing an event's traits to a previously formed stereotype, and, when correspondence is found, assuming that the stereotype is representative of the current event. Applying this heuristic can cause the decision maker to ignore information regarding the commonality, or base rate, of the current event and the sample size that resulted in the current event. Finally, when applying the representative heuristic, individuals tend to lose sight of the fact that extreme events generally regress toward the mean in subsequent sampling. In terms of information security investment decisions, applying the representative heuristic can result in decision makers under or overestimating the financial impact of multiple security events resulting from the same type of threat. For instance, if the decision maker experienced a prior malware infection that caused little damage and was easily eradicated, applications of the heuristic could cause the decision maker to underestimate the impact of a newly detected infection.

Finally, the affective heuristic refers to the unconscious process of relying on one's emotional response regarding an event to guide decision making. Applying the heuristic simplifies the decision process by allowing the decision maker to follow their gut instinct rather than conducting a thorough analysis of the problem domain; however, such a decision strategy can result in significant deviations from rational choice models. In terms of information security investment decisions, the heuristic can result in decision makers overreacting to highly emotional security events.

III. PROSPECT THEORY

Prospect theory provides a simplified description of the way individuals evaluate risky prospects (Kahneman & Tversky, 1979; Tversky & Kahneman, 1981; Tversky & Kahneman, 1992). Numerous tests of the theory show that, when individuals are faced with risk-related decisions, they exhibit different preference patterns for gain-related and loss-related decisions. Specifically, individuals generally choose riskier alternatives when options are discussed in terms of losses, and choose less-risky alternatives when options are discussed in terms of gains.

In one particular test, subjects were shown a short vignette describing the spread of a deadly disease and asked to choose between two hypothetical programs to combat the disease (Tversky & Kahneman, 1981). Half of the subjects were presented with a set of two program options that were both positively framed (i.e., lives saved) and reflected equal expected utility (200 people saved and 400 people die), but one involved more certainty than the other. The other half of the subjects were presented a set of program options that were negatively framed (i.e., lives lost). Again, both options reflected equal expected utility, but one involved more certainty than the other. Table 1 provides the scenario vignette used in the study and the positively and negatively framed option pairs.

Table 1: Classic Prospect Theory Vignette and Framed Options (Adapted from Tversky & Kahneman, 1981)

Vignette: Imagine that the US is preparing for the outbreak of an unusual Asian disease, which is expected to kill 600 people. Two alternative programs to combat the disease have been proposed. Assume that the exact scientific estimates of the consequences of the programs are as follows. Which of the two programs do you favor?	
Positively framed options: **Program A:** 200 people will be saved. (72%) **Program B:** There is a 1/3 probability that 600 people will be saved, and a 2/3 probability that no one will be saved. (28%)	**Negatively framed options:** **Program C:** 400 people will die. (22%) **Program D:** There is a 1/3 probability that nobody will die, and a 2/3 probability that 600 people will die. (78%)

According to rational choice decision making theory, if respondents evaluated the options in a completely rational manner (i.e., the wording had no impact on choice), no significant difference in the positively and negatively framed response patterns should be detected. However, the study's results show that 72 percent of respondents who were shown the positively framed options preferred program A over program B, while 78 percent of respondents who were shown the negatively framed options preferred program D over program C (Tversky & Kahneman, 1981). When faced with positively framed options of equal utility, respondents preferred the more risk-averse option. Saving 200 lives with certainty was strongly preferred over the 1/3 probability of saving 600 lives coupled with the 2/3 probability of saving no lives. However, when faced with negatively framed options, respondents exhibited a different risk posture: they were risk seeking. When negatively framed, subjects strongly preferred the 1/3 probability that no one die coupled with the 2/3 probability that all 600 people die over the more certain scenario of 400 people dying.

Bazerman (2006) notes that framing may explain consumers' propensity for buying insurance and extended warranties even when the cost of such plans exceeds the expected utility. Bazerman describes a study in which half of the subjects were asked to choose between a low probability loss of a very large amount or a certain loss of a much smaller amount, while the other half were asked to choose between the same low probability loss of a very large amount and an insurance premium costing the smaller amount. Interestingly, participants in the second group chose the insurance premium much more frequently than members of the first group chose the certain loss. Bazerman argues that social norms favoring insurance coverage coupled with the availability and vividness of information regarding large, out-of-pocket expenditures that can result from being uninsured cause individuals to overinvest in insurance and extended warranties.

III. EMPIRICAL INVESTIGATION

To empirically determine whether the framing of information security investment requests influences decision makers' preferences, we developed and administered an online survey instrument. Following the example of the classic deadly disease study, the developed instrument contained a short vignette, two investment options, and a request for respondents to indicate which of the two options they preferred. Wording of the vignette closely matched that of the deadly disease study. In the instrument, we randomized the framing selection of investment options so that roughly half of the respondents were shown positively framed options, while the other half were shown negatively framed options. In addition, we randomized the order of investment options in frames. All investment options presented possessed equal expected utility. Table 2 shows the vignette and option sets included in the survey instrument.

<table>
<tr><th colspan="2">Table 2: Information Security Investment Vignette and Framed Options</th></tr>
<tr><td colspan="2"><b>Vignette:</b> Imagine that your company is allocating financial resources to its information security program. Without such investment your company is expected to experience a $600,000 financial impact (asset loss). Note: Your assets include financial resources, intellectual property, organizational reputation, personnel time, and the confidentiality, integrity, and availability of your hardware, software, and data.

Several alternative information security programs to combat the overall threat have been proposed.
Assume the exact scientific estimates of the consequences of the programs are as follows. Please choose your preferred information security program from the set of two choices.</td></tr>
<tr><td><b>Positively framed options:</b>

<b>Program A:</b> $200,000 worth of assets will be saved with certainty.

<b>Program B:</b> There is a one-third probability that $600,000 worth of assets will be saved, and a two-thirds probability that no assets will be saved.</td><td><b>Negatively framed options:</b>

<b>Program A:</b> $400,000 worth of assets will be lost with certainty.

<b>Program B:</b> There is a one-third probability that no assets will be lost, and a two-thirds probability that $600,000 worth of assets will be lost.</td></tr>
</table>

The target population for the study included individuals who have determined or influenced the amount budgeted for information security at the organizational level. Due to this requirement, target subjects could be employed at different organizational levels. Accordingly, we anticipated a wide range of participants from C-level executives to security practitioners.

We sent invitations to participate in the study (via a link to the online survey instrument) to approximately 600 individuals. We do not know the exact number because it involved members of two professional organizations/communities that do not disclose their exact membership roster or size. One was a local InfraGard chapter (http://www.infragard.net) in a large, metropolitan city in the southwestern United States. The other was the Cyber Security and Information Security Subject Matter Expert (SME) group, sponsored by the U.S. Government. We estimated membership at the time of the invitation to be 375 and 125, respectively. Additionally, we sent personal invitations to approximately 100 local area business leaders who participated in an information security training program held in the Southwest US and to our professional contacts.

All email messages specified that respondents needed to have experience determining or influencing the amount budgeted for information security at the organizational level. In the event that a message recipient did not have that level of experience, the email contained a request for the recipient to forward the message on to an individual who did. To ensure that all survey respondents met this requirement, the first question presented asked: "Have you determined the amount, or influenced the decision, of how much money is budgeted for information security at an organizational level?". Respondents who replied yes to this question were then presented with the vignette (Table 2) and a set of either positively or negatively framed investment options. Respondents who replied no to the above question were thanked for their interest in the investigation and exited from the survey.

We obtained 51 responses—a 8.5 percent response rate. This is lower than desired, but not lower than expected for a behavioral science study concerning a sensitive topic and targeting higher-level personnel. Past research suggests information security is a difficult subject to tackle via survey because respondents consider it a sensitive topic area for their organization (Kotulic & Clark, 2004). Of the collected responses, 44 were complete and usable for the study. Twenty of the usable responses were from respondents shown positively framed options (assets saved), whereas the remaining 24 respondents received negatively framed options (assets lost).

Thirty-one (31) of the 44 usable responses came from respondents who provided voluntary demographic data. Relative to the 31 respondents who provided demographic information, the gender split in the sample was 26 males and five females. Although this is not balanced, it reflects the skewed gender distribution in the information security population. The average respondent age was 50 years old. Respondents had 18 years of information security experience on average, so our findings reflect the opinions of highly experienced professionals. Further, respondents had, on average, 12 years of experience directly determining and/or influencing information security budgets, so their opinions are likely to be very insightful. The sample contained individuals from a wide range of job titles, industries, and organization sizes, which Figures 2-4 depict.

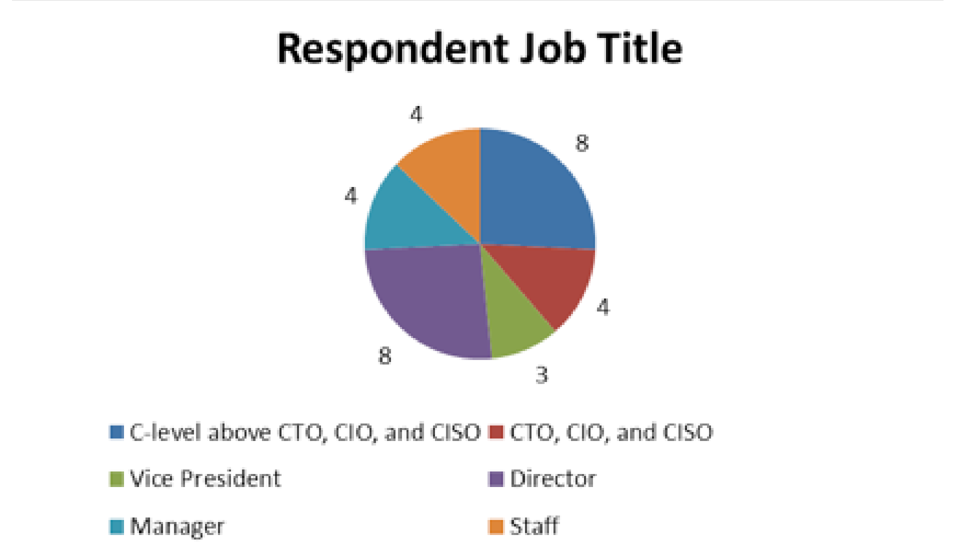

Figure 2: Respondent Title

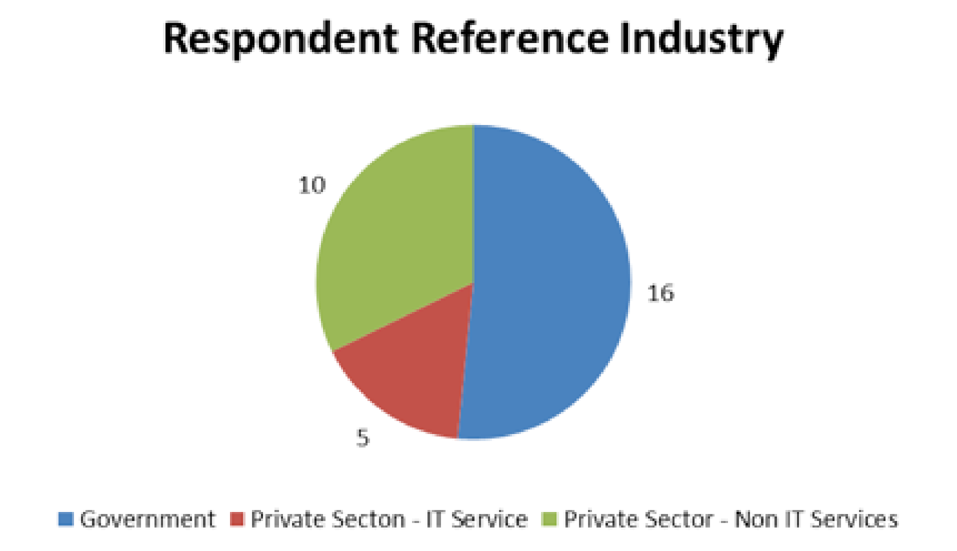

Figure 3: Respondent Industry

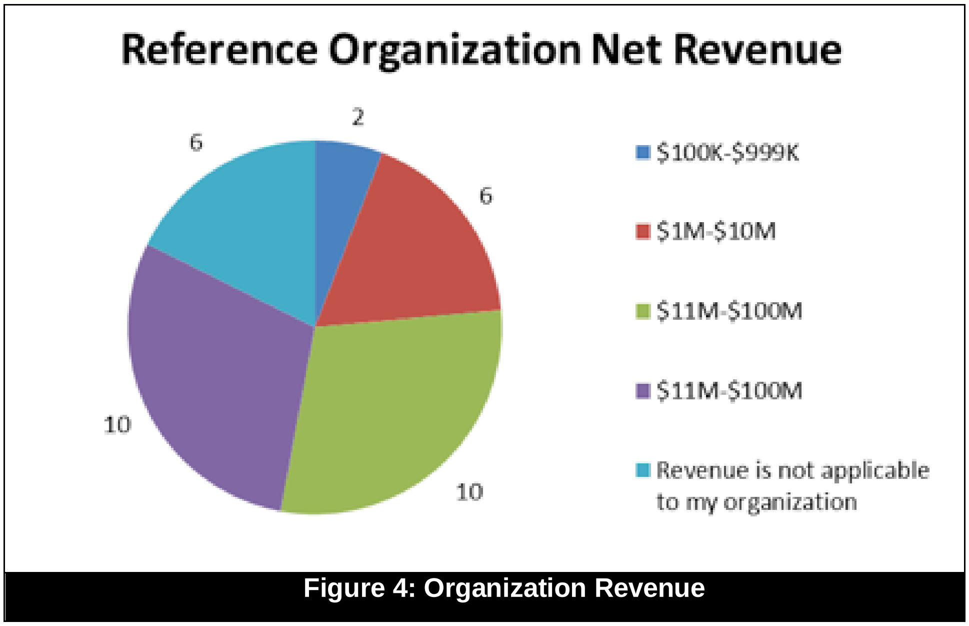

Figure 4: Organization Revenue

IV. FINDINGS

As Table 3 shows, 70 percent of individuals who were shown positively framed information security option choices preferred the more certain option of Program A. In contrast, 83 percent of individuals who were shown negatively framed option choices preferred the riskier option of Program B. To test the statistical significance of these findings, we ran Pearson chi-squared tests of independence to determine whether the differences in positively framed and negatively framed preferences could be due to chance. Results yielded a χ^2 statistic of 12.836 with a significance of $p < .001$.

Table 3. Results

Frame	Selected option A: certain outcome	Selected option B: uncertain outcome
Positive	70%*	30%*
Negative	17%*	83%*
* $\chi^2 = 12.836$, $p < 0.001$		

From these findings, we can observe that decision makers are inclined to take more risks when information security budget requests are framed negatively in terms of the loss-based financial impact to the organization if the requested information security investment is not made. Here, the assets lost are in terms of financial resources, intellectual property, organizational reputation, personnel time, and the confidentiality, integrity, and availability of the organization’s hardware, software, and data. Decision makers who are willing to take more information security risks will presumably invest less in information security.

The survey responses validated our hypothesis that individual information security investment decision makers and information security professionals who influence those decision makers are susceptible to framing biases and do indeed exhibit preference reversals when faced with budget alternatives involving risk. When faced with risk-related decisions positively framed in terms of gains, subjects demonstrated a statistically significant propensity toward risk-aversion. They showed a strong preference for more probabilistically certain options over less certain options. In contrast, when faced with risk-related decisions negatively framed in terms of losses, subjects demonstrated a statistically significant propensity toward risk-seeking behavior. Here, they showed a strong preference for less probabilistically certain options over more certain ones.

We believe this is an important finding because it may partially explain why nearly one in three security practitioners believe that the organization they work for under-funds information security efforts (Richardson, 2011). Based on their knowledge of and constant focus on the information security threat landscape, practitioners are keenly aware of the extent and severity of many information security risks, and of the negative consequences associated with those risks. The cognitive biases resulting from both the availability and representativeness of this information may cause practitioners to over-estimate the probability of incident occurrence and thus the risk of negative consequences from under-investment. Further, the discussions practitioners engage in are often negatively framed: they are focused on prospective losses upon breach rather than prospective gain from security investments. This framing coupled with a biased over-estimate regarding the probability of incident occurrence may in fact lead practitioners to prefer alternatives that lead to an over-investment in security controls. At the same time, however, and perhaps because of increased perception of such biases over time, many managerial decision makers have come to question the validity of the risk data presented to them. This may cause them to be unrealistically optimistic regarding the probability of an incident occurrence and result in those individuals preferring alternatives that under-invest in security controls. Of course, this interpretation is based purely on post-hoc suppositions and further testing is needed to determine if differences in practitioners' and managers' biases and perception frames influence their investment opinions.

Our finding is further significant because negative framing is indeed the way many information security budget requests are presented to organizational decision makers (Buck et al., 2008, Stöwer & Kraft, 2012). Information security professionals often try to convince top management what the negative impact to the organization will be if they do not invest more in information security. In our experience, many senior executives have come to question the reliability and validity of quantified risk data that involves either the probability of the threat and/or the impact of the threat. That, combined with the observed impact of negative framing on managers' decision making process in the context of risk, means security practitioners may be accomplishing the exact opposite of their goal by using negative framing. It serves as a distinct negative bias. Framing the budget request in positive terms—discussing what will be protected instead of what will be lost—may garner greater information security investments in organizations. Information security practitioners and chief information security officers (CISOs) may find this a particularly worthwhile implication of our findings.

However, maximizing information security investments may not be the optimal investment decision for an organization as perceived by its top management. Regardless of potentially competing definitions of what the optimal investment between practitioners and mangers is, true investment optimization must overcome human decision biases. Accordingly, our findings are important to the organizational decision making process itself. They suggest that prevailing information security investment decision models based on rational choice theory and/or economic utility models ought to be supplemented with risk perception measurement and subsequently account for the influence of individual decision biases. Decision makers' perception of risk may be formally modeled in decision support systems used for budgeting to mitigate the perceived risk bias introduced by individuals estimating qualitative budget decision factors.

V. CONCLUDING REMARKS

Admittedly, the information security investment decision is a part of a much larger and complex budget setting process than our vignettes reflect. Anecdotal feedback received during content validation procedures suggests that our low response rate may have been influenced by negative opinions regarding our vignette simplicity. However, we did not attempt to approximate the actual budget process and decision in the survey. If prospect theory's framing effect is not present in information security investment decisions, then any potential bias due to scenario simplicity would equally bias both frames and a significant preference between vignette frames would not be observed. We empirically observed strong framing effects in both frames. Further, we know of no theorized connection between scenario realism and framing effects, and we preferred to model our vignettes after Kahneman and Tversky's Nobel Prize-winning work and scenario format. Further, we believe we obtained a high quality sample from the perspective of level in organizations (>50% of those who provided demographic data were C-level or director-level employees), information security experience (18 years on average), and experience making or influencing information security investment decisions (12 years on average).

In sum, we found that high-level decision makers and information security managers influencing those decision makers do demonstrate preference reversals when evaluating information security investment alternatives. Whereas past literature predominantly focused on rational choice models, our findings suggest that those models could be improved by accounting for prospect theory's framing effects. Our findings suggest that decision makers are typically inclined to take more risks when asked to invest in information security to prevent loss-based consequences. Based on these findings, we conclude that budget requests positively framed in terms of asset protection might garner greater information security investments. We contend that existing information security investment decision models ought to be supplemented with risk perception measurements and account for expected decision biases accordingly.

Future research could empirically explore the following important questions. First, are there conflicting, possibly even off-setting biases involved on the part of information security professions requesting the budget allocations and senior executives determining resource allocations? In our experience, many senior executives no longer believe subjective quantifications of risk probabilities, which may amplify the framing effect. As stated previously, cognitive biases of information security professions that may cause them to tend toward negative framing with potentially exaggerated risks may in fact amplify top management's tendency toward risk-seeking behavior when presented with negatively framed information security budget request justifications. On the other hand, the incidence of several recent, high-profile security breaches may temper that. Further, Bazerman's (2006) findings regarding consumer insurance purchasing patterns might support the notion that information security professionals may essentially be seeking insurance so-to-speak when formulating their budget request. Future research that explores these and other biases involved in the information security budget decision making process is needed. It would also be helpful to empirically examine the subjectivity—its influences and its variation—among information security professionals in estimating parameters required for existing rational choice models based on expected utility theory. This is important for modifying existing prescriptive models to account for framing effect bias, and would further signal the importance of our findings. Last, future research could examine the impact of neutrally framed budget requests—those that discuss both gain and loss prospects.

ACKNOWLEDGEMENTS

The first author thanks the College of Business at the University of Texas at San Antonio for the financial support provided through the Summer Research Grant program.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Bazerman, M. H. (2006). *Judgement in managerial decision making.* Hoboken, NJ: John Wiley & Sons.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78-83.

Buck, K., Das, P., & Hanf, D. (2008). *Applying ROI analysis to support SOA information security investment decisions.* Paper presented at the 2008 Proceedings of the IEEE Conference on Technologies for Homeland Security.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004a). Economics of IT security management: Four improvements to current security practices. *Communications of AIS, 14*, 65-75.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87-92.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investments. *Journal of Management Information Systems, 25*(2), 281-304.

Church, B. K., Libby, T., & Ping, Z. (2008). Contracting frame and individual behavior: Experimental evidence. *Journal of Management Accounting Research, 20*, 153-168.

Crozier, W. R., & Ranyard, R. (1997). Cognitive process models and explanations of decision making. In R. Ranyard, W. R. Crozier, & O. Svenson (Eds.), *Decision making: Cognitive models and explanations* (pp. 5-20). New York: Routledge.

Devers, C. E., McNamara, G., Wiseman, R. M., & Arrfelt, M. (2008). Moving closer to the action: Examining compensation design effects on firm risk. *Organization Science, 19*(4), 548-566.

Edwards, W., Miles, R. F., Jr., & von Winterfeldt, D. (2007). Introduction: Advances in decision analysis from foundations to applications. In W. Edwards, R. F. Miles Jr., & von Winterfeldt, D. (Eds.), *Advances in decision analysis from foundations to applications* (pp. 1-12). New York: Cambridge University Press.

Gordon, L. A. (1989). Benefit-cost analysis and resource allocation decisions. *Accounting, Organizations, and Society, 14*(3), 247-258.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and Systems Security, 5*(4), 438.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM, 49*(1), 121-125.

Herath, H. S. B., & Herath, T. C. (2008). Investments in information security: A real options perspective with Bayesian postaudit. *Journal of Management Information Systems, 23*(3), 337-375.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263-291.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kunreuther, H., Meyer, R., Zeckhauser, R., Slovic, P., Schwartz, B., Schade, C., Luce, M. F., Lippen, S., Krantz, D., Kahn, B., Hogarth, R. (2002). High stakes decision making: Normative, descriptive and prescriptive considerations. *Marketing Letters, 13*(3), 259-268.

Latham, S. F., & Braun, M. (2009). Managerial risk, innovation, and organizational decline. *Journal of Management, 35*(2), 258-281.

Richardson, R. (2011). 2010/2011 Computer crime and security survey. *Computer Security Institute.* Retrieved July 14, 2012, from *http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html*

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavior decision theory. *Annual Review of Psychology, 28*, 1-39.

Stöwer, M., & Kraft, R. (2012). IT security investment and costing emphasizing benefits in times of limited budgets. *Proceedings of ISSE 2012 Securing Electronic Business Processes* (pp. 37-47). Springer.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4481), 453-458.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty, 5*(4), 297-323.

Wagner, T., Hennig-Thurau, T., & Rudolph, T. (2009). Does customer demotion jeopardize loyalty? *Journal of Marketing, 73*(3), 69-85.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research, 19*(1), 106-120.

ABOUT THE AUTHORS

Nicole L. Beebe is an Assistant Professor in the Department of Information Systems & Cyber Security, at the University of Texas at San Antonio (UTSA). UTSA is a National Center of Academic Excellence in Information Assurance for both education and research. She received her Ph.D. in Information Technology from UTSA. She has over fifteen years of experience in information security and digital forensics, from both the commercial and government sectors, and is a Certified Information Systems Security Professional (CISSP). She has published several journal articles related to information security such as *Decision Support Systems* (DSS), *IEEE Transactions of Information Forensics and Security*, *Digital Investigation*, and *Journal of Information System Security* (JISSEC). Her research interests include digital forensics, information security, and data mining.

Diana K. Young is an instructor at the University of Texas at San Antonio and manages the Department of Information Systems and Cyber Security's Advanced Laboratory for Infrastructure Assurance and Security. She received her Ph.D. in Information Technology from UTSA. She has over 15 years of practical IT experience in systems design and development. Her research interest include software development methodologies, security investment decisions, and IS student attraction, engagement, and retention.

Frederick R. Chang is the President of 21CT, Inc., a technology firm based in Austin, Texas. He received his Ph.D. from the University of Oregon. He has published on information security in Science and is the lead inventor on two U.S. patents. He has served as a member of the Computer Science and Telecommunications Board of the National Academies and as a member of the Commission on Cybersecurity for the 44th Presidency.

Communications of the Association for Information Systems

ISSN: 1529-3181