THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

WP # 0041IS-329-2013

Date May 7, 2013

Framing Information Security Budget Requests to Maximize Investments

NICOLE L. BEEBE, Ph.D., CISSP
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
Nicole.Beebe@utsa.edu

DIANA K. YOUNG
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
Diana.Young@utsa.edu

FREDERICK R. CHANG, Ph.D.
21CT, Austin, Texas
fchang@21ct.com

Framing Information Security Budget Requests to Maximize Investments

NICOLE L. BEEBE, Ph.D., CISSP
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
Nicole.Beebe@utsa.edu

DIANA K. YOUNG
Department of Information Systems and Cyber Security
The University of Texas at San Antonio
Diana.Young@utsa.edu

FREDERICK R. CHANG, Ph.D.
21CT, Austin, Texas
fchang@21ct.com

Abstract:

Nearly one in three security practitioners believe that the organization they work for under-funds information security efforts. Rational choice and economic models have been developed to help decision makers determine the optimal amount they should spend to protect a set of information assets. These models presume investment decisions are rationally made, despite long-standing behavioral and decision making research to the contrary that shows decisions are not entirely rational when risk and uncertainty are involved. The purpose of this research was to empirically validate our hypothesis that information security investment decision makers exhibit irrational decision making behavior when faced with competing budget alternatives involving risk. 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. The results of an on-line survey empirically validates our hypothesis that information security investment decision makers in fact exhibit irrational decision making behavior when faced with competing budget alternatives involving risk. High-level decision makers exhibit irrational decision making behavior concerning information security when faced with competing budget alternatives involving risk. The findings suggest that justifying budget requests in terms of *assets protected* will often garner greater budgets than those framed in terms of the negative ramifications if security investments are not made. The findings also suggest that existing rational choice and economic models for information security investments should be augmented with measurement of risk perception and account for expected decision biases.

Keywords: Information Security, Prospect Theory, Framing Effect, Investment, Risk

JEL Classification Codes: D81, M19

Introduction

Information security is concerned with protecting the confidentiality, integrity, and availability of information systems against security exploits targeted at vulnerabilities within those systems. To achieve this goal, organizations implement controls to: protect information assets against threats, detect when security incidents occur, and correct damages resulting from successful security exploits. Controls may involve use of technologies, human resources, processes, training, and other initiatives to combat against security threats.

Recent research indicates that implemented controls may be reducing the effectiveness of certain security exploits.[11] Fewer organizations are reporting incidents of device theft, insider abuse, denial of service, financial fraud, password sniffing, and wireless networks exploits. However, incidents of involving botnets, malware infections, and phishing are increasing. This indicates that organizations need to implement additional controls and/or improve upon existing controls to thwart against these and other newly identified security threats.

Efforts aimed at improving an organization's security posture generally require monetary investments to fund the development of necessary controls. However, nearly one in three security practitioners believe that the organization they work for under-funds information security efforts.[11] Accordingly, two key challenges facing information security professionals are determining how much they should spend on security initiatives and 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 a set of information assets.[1-4, 6, 8, 15] 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. Unfortunately, security benefits are often difficult to quantify making application of these models difficult. Accordingly, some practitioners use a modified approach; examining costs and benefits but placing less emphasis on the formal quantification of benefits.[7] In addition, some information security practitioners rely on past year's budgets, industry best practices, and business requirements to drive information security investment requests.

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 must consider information security investment requests amidst competing funding requests across the organization, with a limited pool of available funds. Accordingly, many factors, including qualitative considerations, impact manager's investment decisions.[5] 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 decisions are not entirely rational when risk and uncertainty are involved.[9, 12] There is little certainty in information security. Some say the only certainty is "*when, not if*"—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 elsewhere. Under-investment risks security of information, productivity, and stakeholder confidence in the organization.

Past normative decision making models for information security may be improved by accounting for the impact of risk perceptions on otherwise rational decisions. The purpose of this research was to empirically validate our hypothesis that information security investment decision makers exhibit irrational decision making behavior when faced with competing budget alternatives involving risk. 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.[9] Prospect Theory research has shown 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.

Based on this and the fact that top managers consider both qualitative and quantitative factors when making investment decisions,[5] 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 intended. 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 this irrationality 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 question, we conducted a scenario based, empirical study of the information security investment decisions made by information security managers and executives.

Prospect Theory

Prospect Theory provides a simplified description of the way individuals evaluate risky prospects.[9, 13, 14] Central to the theory is the concept of framing, the manner in which a statement or question is posed to a decision maker. 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.

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.[13] Half of the subjects were presented with a set of two program options that were both *positively framed* (i.e. lives saved), reflected equal expected utility (200 people saved and 400 people die), yet 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, yet one involved more certainty than the other. Table 1 provides the scenario vignette used in the study as well as the positively and negatively framed option pairs.

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, results of the study showed that 72% of respondents who were shown the positively framed options, preferred program A over program B, while 78% of respondents who were shown the negatively framed options, preferred program D over program C.[13] 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.

Table 1: Classic Prospect Theory Vignette and Framed Options Adapted From [13]

Vignette: Imagine that the U.S. 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:	**Negatively Framed Options:**
Program A: 200 people will be saved. (72%)	**Program C:** 400 people will die. (22%)
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%)	**Program D**: There is a 1/3 probability that nobody will die, and a 2/3 probability that 600 people will die. (78%)

Empirical Investigation

To empirically determine if framing of information security investment requests influences decision makers' preferences, we developed and administered an on-line survey instrument. Following the example of the classic deadly disease study,[13] 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. Within the instrument, the framing of investment options was randomized, so that roughly half of the respondents were shown positively framed options, while the other half were shown negatively framed options. In addition, the order of investment options within frames was randomized. All investment options presented possessed equal expected utility. Table 2 shows the vignette and option sets included in the survey instrument.

Table 2: Information Security Investment Vignette and Framed Options

Vignette: 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.	
Positively Framed Options:	**Negatively Framed Options:**
Program A: $200,000 worth of assets will be saved with certainty.	Program A: $400,000 work of assets will be lost with certainty.
Program 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.	Program 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.

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.

Invitations to participate in the study along with a link to the online survey instrument were sent to approximately 600 individuals. The exact number is not known, as 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 southwest United States. The other was the Cyber Security and Information Security Subject Matter Expert (SME) group, sponsored by the U.S. government. Membership at the time of the invitation was estimated at 375 and 125 respectively. Additionally, the research team sent personal invitations to approximately 100 local area business leaders who participated in an Information security training programs held in the Southwest U.S., as well as professional contacts of the research team.

All email messages specified that respondents should 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 (Table2) and a set of either positively or negatively framed investment options. Respondents, who replied no to the above question, were thanked for their interested in the investigation and exited from the survey.

We obtained fifty-one (51) responses—a 8.5% 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, as respondents consider it a sensitive topic area for their organization.[10] Of the collected responses, 44 were complete and usable for the study. Twenty (20) 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, 5 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 12 years of experience directly determining and/or influencing information security budgets, so their opinions are very insightful. The sample contained individuals from a wide range of job titles, industries, and organization sizes, which is depicted in Figures 1 - 3.

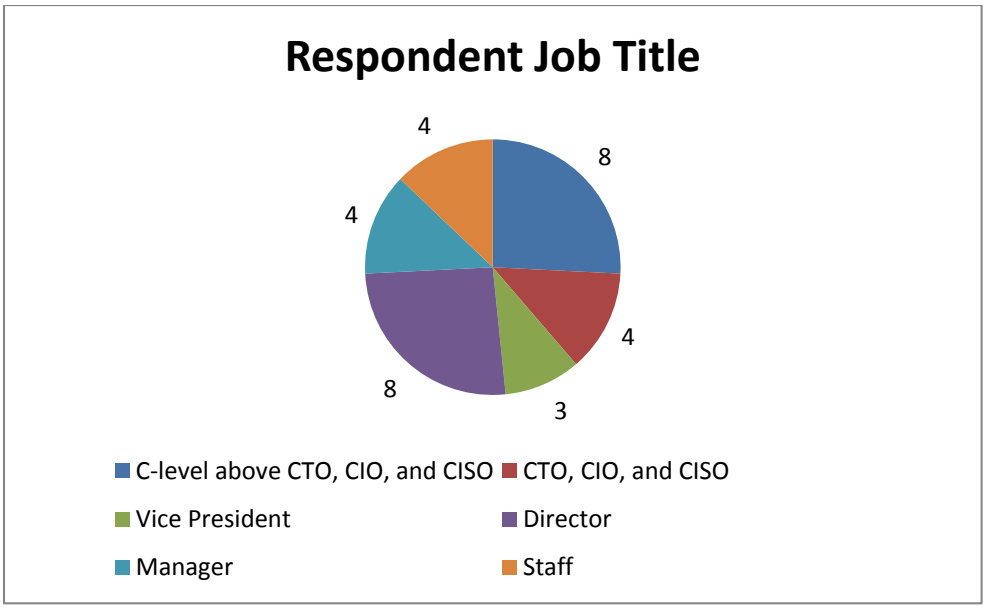

Figure 1: Respondent Title

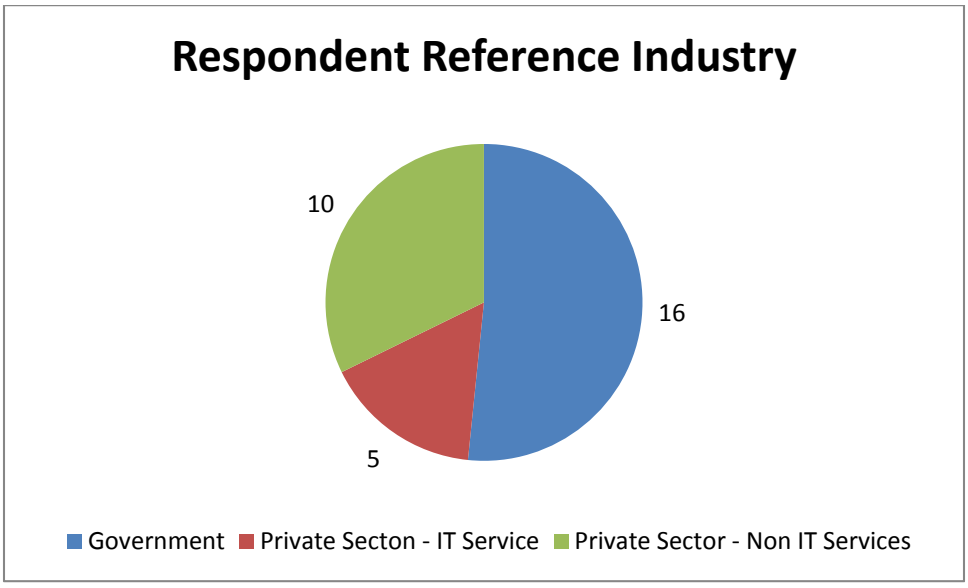

Figure 2: Respondent Industry

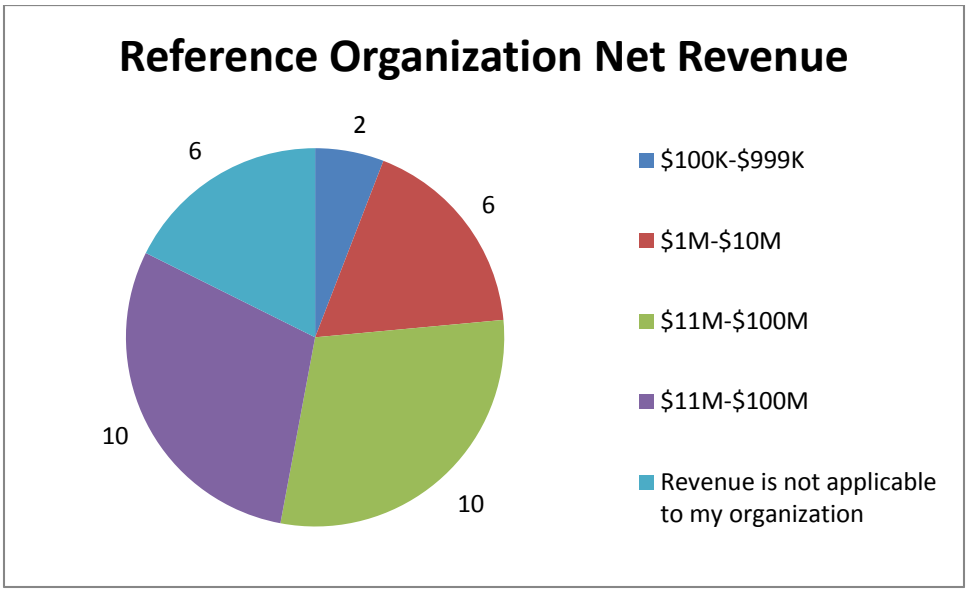

Figure 3: Organization Revenue

Findings

The survey responses validated our hypothesis that information security investment decision makers do exhibit irrational decision making behavior when faced with competing budget alternatives involving risk. When faced with risk related decisions positively framed in terms of gains, individuals demonstrated a statistically significant propensity toward risk-aversion, showing 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, individuals demonstrated a statistically significant propensity toward risk-seeking behavior. Here, they showed a strong preference for less probabilistically certain options over more certain ones.

Specifically, as Table 3 shows, 70% of individuals who were shown positively framed information security option choices preferred the more certain option of Program A. In contrast, 83% 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 test of independence to determine if 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 < .001. This indicates that there is less than a 1 in 1000 chance that the correspondence between the framing and preferences observed were due to chance.

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 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 your hardware, software, and data. Decision makers who are willing to take more information security risks will presumably invest less in information security. This is an important finding, because it may explain, at least in part, why nearly one in three security practitioners believe that the organization they work for under-funds information security efforts.[11] It is also significant because, in our experience, this negative framing is indeed the way most information security budget requests are currently framed. Information security professionals continually try to convince top management what the negative impact to the organization will be if they do not invest more in information security. Perhaps, simply framing the budget request in positive terms, discussing what will be protected instead of what will be lost, will garner greater information security investments within organizations.

These findings are also important for top management. Acknowledging that their perception of information security risk may be clouding their decision making in a non-rational manner may improve the veracity of their rational choice based budget decision. Further, decision maker perception of risk may be modeled in decision support systems used for budgeting to remove, or at least lessen the perceived risk related bias introduced by individuals estimating qualitative budget decision factors.

Concluding Remarks

Admittedly, the information security investment decision is a part of a much larger and complex budget setting process than is reflected in our vignettes. 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.

Last, while our findings are from a smaller than desired sample size, we believe we obtained a high quality sample from the perspective of level within the organization (>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 quality, high-level decision makers and information security managers influencing those decision makers do demonstrate irrationality when evaluating information security investment alternatives. Whereas past literature predominantly focused on rational choice models, our findings suggest that those models could be improved if Prospect Theory's framing effects were accounted for. 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 asset protection might be more successful in the future, than their more commonly, negatively framed counterparts that warn of what may happen without sufficient organizational investment in information security.

Acknowledgement

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

1. Bodin, L. D., Gordon, L. A. and Loeb, M. P. Evaluating Information Security Investments Using the Analytic Hierarchy Process. *Communications of the ACM*, *48*, 2 (2005) 78-83.
2. Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. Economis of It Security Management: Four Improvements to Current Security Practices. *Communications of AIS*, *14* (2004) 65-75.
3. Cavusoglu, H., Mishra, B. and Raghunathan, S. A Model for Evaluating It Security Investments. *Communications of the ACM*, *47*, 7 (2004) 87-92.
4. Cavusoglu, H., Raghunathan, S. and Yue, W. T. Decision-Theoretic and Game-Theoretic Approaches to It Security Investments. *Journal of Management Information Systems*, *25*, 2 (2008) 281-304.
5. Gordon, L. A. Benefit-Cost Analysis and Resource Allocation Decisions. *Accounting, Organizations, and Society*, *14*, 3 (1989) 247-258.
6. Gordon, L. A. and Loeb, M. P. The Economics of Information Security Investment. *ACM Transactions on Information and Systems Security*, *5*, 4 (2002) 438.
7. Gordon, L. A. and Loeb, M. P. Budgeting Process for Information Security Expenditures. *Communications of the ACM*, *49*, 1 (2006) 121-125.
8. Herath, H. S. B. and Herath, T. C. Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems*, *23*, 3 (2008) 337-375.
9. Kahneman, D. and Tversky, A. Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*, 2 (1979) 263-291.
10. Kotulic, A. G. and Clark, J. G. Why There Aren't More Information Security Research Studies. *Information & Management*, *41*, 5 (2004) 597-607.
11. Richardson, R. 2010/2011 Computer Crime and Security Survey. *Computer Security Institute. Available at: http://analytics. informationweek. com/abstract/21/7377/Security/research-2010-2011-csisurvey. html (Accessed: 14 July 2011)* (2011).
12. Slovic, P., Fischhoff, B. and Lichtenstein, S. Behavior Decision Theory. *Annual Review of Psychology*, *28* (1977) 1-39.
13. Tversky, A. and Kahneman, D. The Framing of Decisions and the Psychology of Choice. *Science*, *211* (1981) 453-458.
14. Tversky, A. and Kahneman, D. Advances in Prospect Theory: Cumumlative Representation of Uncertainty. *Journal of Risk and Uncertainty*, *5* (1992) 297-323.
15. Wang, J., Chaudhury, A. and Rao, H. R. A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, *19*, 1 (2008) 106-120.