Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Investment in Information Security Measures: A Behavioral Investigation

Roozmehr Safi
Texas Tech University

Glenn Browne
Texas Tech University

Investment in Information Security Measures: A Behavioral Investigation

Research in Progress

Roozmehr Safi
Texas Tech University, Lubbock, Texas, USA {r.safi@ttu.edu}

Glenn J. Browne
Texas Tech University, Lubbock, Texas, USA {glenn.browne@ttu.edu}

ABSTRACT

In a pilot study, we employed a series of novel economic games to investigate the underexplored behavioral aspects of security investment decisions and security investment structure decisions (i.e., budgeting the security expenditure among different types of security measures). In our study, decision makers exhibited a bias toward investing in prevention even though investing in detection and response yielded the same return on security investment. We also demonstrated that it is difficult for human decision makers to determine the optimal security investment amount even when return on investment is readily calculable. Nearly all participants invested in security when the risk was so small that the economically justifiable security investment amount was zero.

Keywords: Information Security, security investment, prevention, detection

INTRODUCTION AND PROBLEM STATEMENT

As we rely more on information systems, security incidents are becoming more and more frequent and costly. To mitigate risk, both individuals and organizations invest money to acquire security measures. Similar to any other investment, the amount of investment in security may be inadequate, adequate, or even in excess with respect to the context. Although analytical methods can help decision making in the domain of security investment, individuals' (subjective) decisions play a key role in this area. Despite the prominent role that subjective opinions play in security decisions, the behavioral aspects of security investment have been largely ignored by the literature.

Apart from the total amount of security investment, the “security investment structure”, or the way the security budget pie is divided, can also greatly impact the effectiveness of a security solution (Cavusoglu, Mishra, & Raghunathan, 2004). Two major areas of security investment are “prevention” and “detection and response” (a.k.a., “correction”). As it turns out, finding the right structure, or mix, of these types of security measures is very challenging in practice. For example, a recent study based on 20 years of data has shown that security decision makers in companies have long overspent on prevention technologies and underspent on detection and response technologies (Gartner Security & Risk Management Summit, 2014). The observed deviations from the optimal security investment structure may partly be explainable using behavioral decision theories, as research performed over the past few decades has provided solid evidence that behavioral factors play a prominent role in assessing, perceiving, and mitigating risk (Slovic, 2010).

In our study, we developed an experiment that involves a series of novel economic games. We use this experiment to evaluate subjects’ investment decisions in security and compare it to the “correct,” optimal invest amount to determine the optimality of security investment decisions. Our experiment allows participant to invest in preventative security measures, in detective security measures, or in a mixture of the two. The experiment is designed in a way that yields the exact same level of return on security investment for either type of measure or for a mix of them. This allows us to establish empirically whether individuals are inherently biased toward prevention, as the real world investment data seem to show.

Our study is concerned with security investment decisions made at the individual level. Home users as well as many organizational users make their security investment decisions autonomously. Nevertheless, we must acknowledge that security investment decisions at the organizational level are typically transcend individuals. But even those decisions are formed by individuals, which makes the study of individual-level decisions valuable for understanding organizational-level decisions as well (Beebe, Young, & Chang, 2014).

SECURITY RISK, ITS MEASUREMENTS, AND SECURITY INVESTMENT

Traditional risk or decision analysis models are the most widely used methods to find optimal investment values. These methods are primarily based on their expected value (EV) (Gordon & Loeb, 2002; Hoo, 2000). The use of EV in security investment can be traced back to 1979[1]. This method calculates the total cost of security by identifying the major areas of vulnerability, the likelihood of incidents in those areas, and their costs. A fundamental assumption of IS security investment models based on EV is that decision makers are indifferent between scenarios that lead to the same expected values (Gordon & Loeb, 2002). This assumption, however, is frequently violated in everyday decision making (Tversky & Kahneman, 1986). Our aim is to demonstrate the existence of these biases in the domain of information security investment.

HYPOTHESES

Security risk has two cost components of two different types: an *expected* cost of security incidents themselves and an *immediate* cost that companies incur by acquiring security measures. Owners of information systems make decisions about investing monetary resources (incurring a sure loss) to lower the expected, risky cost component. Prospect theory (Tversky & Kahneman,

[1] National Bureau of Standards, Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65 (Washington, DC: U.S. General Printing Office, 1979).

1986) can help us analyze decisions made in risky situations such as this. According to this theory, the process of decision making under risk starts with an editing phase during which prospects are coded as either gains or losses (Kahneman & Tversky, 1979). We propose that presenting security as either prevention or detection can affect the outcome of this phase and consequently result in different security investment decision outcomes. Prevention is a "pre-event" or a "prognostic" activity. Detection is "post-event" or a "diagnostic" activity; it is about finding out about something bad that has happened (e.g., a server that has been compromised). Accordingly, when thinking about detection, subjects already envision themselves in the domain of losses. Kahneman and Tversky (1984) have shown that decision makers are more risk-seeking when losses are made salient. We propose that when deciding on how much to spend on detection, decision makers opt for taking more risk (e.g., less investment in security) compared to when they make decisions about prevention. Accordingly we propose that subjects have a higher propensity to spend on prevention than on detection

H1: When given a chance to buy a mix of prevention and detection, preventative measures take up a larger share of the total security expenditure.

The typical person is risk averse for gains. That is why people usually spend more than the expected cost of incidents to buy insurance, as insurance is framed as a gain and as a socially responsible and desirable behavior by insurance companies. To determine how much one *should* spend on insurance, one can use the expected loss from incidents as the reference point. For example, if the expected loss is estimated to be $10,000, then an average person should be willing to pay some amount more than this expected loss as an insurance premium. Counterintuitively, the maximum amount one should pay to *buy* security measures (i.e., to self-insure) is in most cases just a fraction of the expected amount of loss due to incidents. For two broad classes of information security breach probability functions, this amount has been shown to be less than 37% of the expected loss due to incidents (Gordon & Loeb, 2002). Accordingly we hypothesize that:

H2-A: In general, subjects tend to invest more than the optimal investment amount to guard against threats.

H2-B: Subjects tend to invest in security even in situations in which the risk of incidents is very low, and thus does not economically warrant any security investment.

THE EXPERIMENT

To study our hypotheses we designed an experiment comprised of three novel one-period economic security games. Twenty-one undergraduate business students participated in the pilot study for course credit and monetary reward. Participants used laptop computers to browse to a website developed for this study by the experimenters. Subjects were told that they could earn up to $20 in cash based on the optimality of their security investment decisions. The experiment was comprised of three sections. In all three sections subjects were told that their job was to protect a certain dataset with a known value of $10,000 that was subject to security incidents with a known chance of occurrence. In Section 1 (prevention-only game), subjects could reduce the chance of losing their data by half for every $1,000 that they spent on a preventative measure. In Section 2 (detection-only game), subjects could reduce the chance of losing their data by half for every $1,000 that they spent on a detective measure. Finally, in Section 3 (prevention and detection game), subjects could use either or both methods to reduce the chance of losing data. Sections 1 and 2 had six security scenarios each with different chances of incidents occurring and Section 3 had eight security scenarios. As explained earlier, the game is designed in a way that yields the exact same expected return on security investment irrespective of the investment structure. Participants could input different investment amounts and then use a “risk calculator” to see the resulting risk level before submitting their answers. Therefore, subjects could readily see the (expected) effect of their investment. The order of sections was counter-balanced.

PRELIMINARY ANALYSIS AND RESULTS

We matched and compared subjects’ answers to equivalent questions from Section 1 and Section 2. The McNemar's exact test statistic for paired proportions does not show any significant difference between security investments. We also conducted a paired-sample t-test between answers in Section 1 and corresponding answers in Section 2 but the difference was not statistically significant (t(124) =0.64, P = 0.52). We used the answers in Section 3 to test H1. We conducted a paired-sample t-test between investment amount in prevention and investment amount in detection in every scenario. There was a significant difference between investment in prevention (mean: $1,994, SD: $1,477) and investment in detection (M: $1,412, SD: $1,177); t(167)=4.053, P < .001, indicating that participants favored prevention over detection when both investment options were available. In an overwhelmingly large number of cases (84%) individuals invested in excess of the optimal amount. Participants spent, on average, $1,347 (SD=$1,948) more than the optional amount, which was significantly different from zero (t(422)=14.15, P < .001), supporting H2-A. More surprisingly, subjects invested in 95% of the scenarios in which risk was so small that the optimal investment amount was zero, supporting H2-B.

DISCUSSION

Organizations are increasingly becoming aware of the fact that security is no longer an IT issue but rather is an enterprise-level risk issue. Accordingly, investing in security is becoming increasingly important and complicated. Improving these decisions would not be possible without developing a deep understanding of the possible behavioral factors that may affect security investment and budgeting decisions. In this paper we used a series of novel economic games to study security investment decisions from a behavioral decision making perspective. In a controlled laboratory setting we were able to demonstrate that given the same return on security investment, decision makers exhibit a tendency, or a bias, toward spending on prevention rather than detection when given the option. We also demonstrated that it is difficult for human decision makers to determine the optimal security investment value even when return on security investment is readily calculable. Participants in our experiment heavily overinvested in security measures in magnitudes that cannot be attributable to risk aversion alone. In fact, nearly all of our participants invested money in security when the risk was so small that the economically justifiable security investment amount was zero. Overall, our results provide preliminary yet striking evidence that such biases play a significant role in security investment decisions. These preliminary results warrant conducting future research using a larger number of participants as well user users with different levels of wok experience to explore the robustness of this behavioral bias. We believe this is an underexplored area that merits substantial amounts of further research.

References:

Beebe, N. L., Young, D. K., and Chang, F. R. 2014. “Framing Information Security Budget Requests to Influence Investment Decisions.” *Communications of the Association for Information Systems* (35:1), pp. 7.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. “A Model for Evaluating IT Security Investments.” *Communications of the ACM* (47:7), pp. 87-92.

Gordon, L. A., and Loeb, M. P. 2002. “The Economics of Information Security Investment.” *ACM Transactions on Information and System Security (TISSEC)* (5:4), pp. 438-457.

Hoo, K. J. S. 2000. *How much is enough? A risk management approach to computer security.*Working Paper, Stanford University.

Kahneman, D., and Tversky, A. 1979. “Prospect theory: An analysis of decision under risk.” *Econometrica: Journal of the Econometric Society* (4:2), pp. 263-291.

Kahneman, D., and Tversky, A. 1984. “Choices, values, and frames.” *American psychologist,* (39:4) pp. 341-350.

Slovic, P. 2010. *The feeling of risk: New perspectives on risk perception.* Routledge.

Tversky, A., and Kahneman, D. 1986. "Rational Choice and the Framing of Decisions." *Journal of Business* (59:4) pp. 251-278.