6-2017

The Impact of Monetary Value Gains and Losses on Cybersecurity Behavior

Samuel Noah Smith
Missouri University of Science and Technology, snsww4@mst.edu

Fiona Fui-Hoon Nah
Missouri University of Science and Technology, nahf@mst.edu

Maggie Cheng
New Jersey Institute of Technology, maggie.cheng@njit.edu

Santhosh Kumar Ravindran
Missouri University of Science and Technology, srkd5@mst.edu

The Impact of Monetary Value Gains and Losses on Cybersecurity Behavior

Samuel Noah Smith
Missouri University of Science and Technology
snsww4@mst.edu

Fiona Fui-Hoon Nah
Missouri University of Science and Technology
nahf@mst.edu

Maggie X. Cheng
New Jersey Institute of Technology
maggie.cheng@njit.edu

Santhosh Kumar Ravindran
Missouri University of Science and Technology
srkd5@mst.edu

ABSTRACT

This research examines if users take more risky cybersecurity actions when presented with the possibility of losing monetary value rather than gaining monetary value. Prospect theory provides the theoretical foundation for the research. An experimental design is proposed to test the hypothesis for the research.

Keywords

Cybersecurity, behavior, gains, losses, monetary value, prospect theory

INTRODUCTION

Users are commonly referred to as the "weakest link in the security chain" (Sasse et al., p. 122). Although a computer security system may comprise advanced technology designed to protect the underlying architecture of an information system, the unpredictable and uncontrollable behavior of users may infringe the ability of the security system to provide protection. For instance, a highly-advanced firewall will not benefit a system if users neglect to keep the firewall enabled. Hence, the human factor is a vital component—and potential area of exploitation—for a computer security system.

Frequently, users must practice their own judgement when determining how to respond to a situation involving cybersecurity, such as when presented with a phishing email. Lack of knowledge (Chan & Mubarak, 2012), malicious intent (Warkentin & Willison, 2009), and even personality traits (Warkentin et al., 2009) could influence the user's assessment of and response to a situation in a cybersecurity context. Although previous behavioral information security research has explored a number of factors which could impact the user's behavior in information security, research is warranted to gain a better understanding of the human component so that we can mitigate weaknesses caused by undesirable user behavior.

In this research, we are interested to understand users' cybersecurity behavior in the context where they are offered a monetary gain vs loss. Given the importance of personal finance, and the ease at which it can be identified with, we believe that exploring such a topic will contribute meaningful findings to the behavioral information security research domain. Our research will primarily be guided by the following research question:

"Are users more willing to take greater risks in a cybersecurity context when gains and losses of monetary value for their risky behavior are involved?"

LITERATURE REVIEW

A review of the literature shows that risk perception is a factor which users consider when determining a course of action. In the information security domain, Farahmand & Spafford (2013) state that individuals within an organization (i.e., insiders) may be deterred from undesirable information security behaviors by reducing their motivation to misbehave and conveying that attempts to misbehave will present too much risk. Shoshitaishvili et al. (2014) analyzed a competition in which teams competed in cybersecurity challenges. Some tasks presented a level of risk to the teams, and it was found that teams were

willing to engage in riskier tasks if those tasks provided higher rewards, measured in terms of competition points (Shoshitaishvili et al., 2014). In other words, the teams were willing to engage in riskier behavior when they perceived a higher level of reward as a result of their actions.

Framing, which refers to how information is presented, also shows up in the literature as a factor which influences users' cybersecurity behavior. Beebe et al. (2014) surveyed industry professionals to understand their decision-making processes when responding to information security budget requests. Their findings suggest that these decision makers may be more inclined to take risks when they are presented with information security budget requests that emphasize the financial losses (i.e., negative framing) that will impact the organization if the budget requests are not met (Beebe et al., 2014). Home computer users are more likely to commit a security behavior when they are provided with a message that focuses on the positive outcomes of performing the behavior, rather than the negative outcomes of not performing the security behavior (Anderson & Agarwal, 2010). Hence, users may perform cybersecurity actions depending on how the potential gains or potential losses that would result from the actions are presented to them.

User characteristics and their potential relationship with risky cybersecurity behavior have been explored by researchers. Warkentin et al. (2012) examined how personality characteristics relate to the intention to commit computer abuse. Their results suggest that users with higher levels of conscientiousness are more concerned with reprimand that could result from stealing data than less conscientious users; and users with high levels of neuroticism and openness pay closer attention to the costs required to perform protective security actions than users with low levels of neuroticism and openness (Warkentin et al., 2012). Halevi et al. (2013) explored the potential relationship among personality traits and users' cybersecurity and privacy behavior; their results suggest that higher levels of openness are related to a higher tendency to share private information online, which may result in a higher vulnerability of information leakage. Hu et al. (2015) utilized a cognitive neuroscience approach when researching the role of self-control in cybersecurity violations. Their findings show that variations in the user's level of self-control demonstrate significant differences in their information security behavior, which can be shown by the user's neural activities (Hu et al., 2015). Hence, there may be a relationship between user characteristics and risky information security behavior.

THEORETICAL FOUNDATION AND HYPOTHESIS

Prospect theory, which originated within behavioral economics research, will play a fundamental role in our research. Prospect theory describes the way people choose between courses of actions when they are under a state of threat, and where the probability of an outcome is known (Tversky & Kahneman, 1984). The decision-making process for determining a course of action becomes challenging for users when the available choices may conflict with their objectives. The manner in which information is conveyed to the user (i.e., framing) may influence their judgements and decisions (Tversky & Kahneman, 1984).

According to prospect theory, choices are made in two phases (Farahmand & Spafford, 2013). During the first phase, the individual assesses the levels of risk involved with each course of action, and then they subjectively determine if the course of action will provide a gain or a loss. During the second phase, the individual assesses each option and then chooses the course of action with the highest utility, measured in terms of gains or losses. Prospect theory states that a loss is perceived to be more substantial than a benefit of the same degree (Tversky & Kahneman, 1984). In other words, a potential loss is preferred over a guaranteed loss, while a guaranteed gain is preferred over a potential gain (Tversky & Kahneman, 1986). Hence, individuals tend to react more strongly to a message which conveys a loss rather than a message which conveys a gain.

For example, Tversky & Kahneman (1981) conducted an experiment where participants were presented with a scenario in which they had to make a decision regarding an outbreak of a disease that was estimated to kill 600 people. Participants had to choose between four courses of action. Two of the options were positively framed, and two of the options were negatively framed. The positively framed options were: (A) 100% chance that 200 people will be saved, and (B) 1/3 probability that 600 people will be saved, and 2/3 probability that no people will be saved. The negatively framed options were: (C) 100% chance that 400 people will die, and (D) 1/3 probability that nobody will die, and a 2/3 probability that 600 people will die. 72% of the participants who were presented with the positively framed options chose option A over option B, which indicates a

preference toward the guaranteed saving of 200 lives rather than the possible saving of all 600 lives (i.e., risk-averse behavior). 78% of the participants who were presented with the negatively framed options chose option D over option C, which indicates a preference toward the possible prevention of losing all 600 lives rather than the guaranteed prevention of losing 200 lives (i.e., risk-seeking behavior).

Based on prospect theory, we hypothesize that users are more willing to take risky cybersecurity actions to avoid losses (fear) than to benefit from gains (benefit). For example, individuals tend to react more strongly to a message which conveys a loss rather than a message that conveys a gain (Tversky & Kahneman, 1984). Because users value preventing losses more than benefitting from gains (even if the amount of gains and losses is controlled for and kept constant), we hypothesize that they will take more risk in cybersecurity in the former case than the latter case. Hence, we propose the following hypothesis:

> H1: Users are more likely to engage in risky computer security actions when they will result in the prevention of losing monetary value as compared to gaining monetary value.

RESEARCH METHODOLOGY

A between-subjects experimental study is proposed to assess users' cybersecurity behaviors in the context of gaining versus losing monetary value in downloading a browser plugin that may threaten computer security. Hence, there are two conditions in the experiment, where the first condition poses the need for a browser plugin download that will help to prevent losing all of one's university account credits, which are used for university purchases, whereas the second condition poses the need for a browser plugin download in order to double one's university account credits. In other words, the first condition minimizes any losses, whereas the second condition offers monetary gains.

Subjects from a midwestern university will be recruited for the experiment. The subjects will be randomly assigned to one of the two experimental conditions and will be posed with the request to download a browser plugin in that condition, after which they will select whether to download the plugin or not.

EXPECTED CONTRIBUTIONS AND CONCLUSION

This research assesses the degree to which the gains and losses of monetary value will affect one's cybersecurity behavior. Based on prospect theory, we believe that offering incentives in the form of gains and losses can affect users' cybersecurity behavior and hence, users may need to be trained about assessing cybersecurity risks independent of the incentives posed to them, which is an irrelevant factor to cybersecurity risks.

REFERENCES

1. Sasse, M., Brostoff, S., and Weirich, D. (2001) Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security, *BT Technology Journal*, 19, 3, 122-131
2. Chan, H. and Mubarak, S. (2012) Significance of Information Security Awareness in the Higher Education Sector, *International Journal of Computer Applications,* 60, 10, 23-31
3. Warkentin, M. and Willison, R. (2009) Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems*, 18, 101-105
4. Shropshire, J., Warkentin, M. and Sharma, S. (2015) Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, *Computers & Security*, 49, 177-191
5. Farahmand, F. and Spafford, E. (2013) Understanding insiders: An analysis of risk-taking behavior, *Information Systems Frontiers*, 15, 5-15
6. Shoshitaishvilli, Y., Invernizzi, L., Doupe, A., and Vigna, G. (2014) Do You Feel Lucky? A Large-Scale Analysis of Risk-Rewards Trade-Offs in Cyber Security, *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, 1649-1656
7. Beebe, N.L., Young, D.K., and Cheng, F.R. (2014) Framing Information Security Budget Requests to Influence Investment Decisions, *Communications of the Association for Information Systems*, 35, 7, 133-143
8. Anderson, C.L., and Agarwal, R. (2010) Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions, *MIS Quarterly*, 34, 3, 613-643

9. Warkentin, M., McBride, M., Carter, L., and Johnston, A. (2012) The Role of Individual Characteristics on Insider Abuse Intentions, *Americas Conference on Information Systems 2012 Proceedings,* 28, 1-10
10. Halevi, T., Lewis, J., and Memon, N. (2013) A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits, *Proceedings of the 22nd International Conference on World Wide Web,* 737-744
11. Hu, Q., West, R., and Smarandescu, L. (2015) The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective, *Journal of Management Information Systems,* 31, 6-48
12. Tversky, A. and Kahneman, D. (1984) Choice, Values, and Frames, *American Psychologist,* 39, 4, 341-350
13. Tversky, A. and Kahneman, D. (1986) Rational Choice and the Framing of Decisions, *The Journal of Business,* 59, 4, 251-278
14. Tversky, A. and Kahneman, D. (1981) The Framing of Decisions and the Psychology of Choice, *Science,* 211, 4481, 453-458