5-2018

Effect of Probable and Guaranteed Monetary Value Gains and Losses on Cybersecurity Behavior of Users

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

Effect of Probable and Guaranteed Monetary Value Gains and Losses on Cybersecurity Behavior of Users

Santhosh Kumar Ravindran
Missouri University of Science and Technology
srkd5@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

ABSTRACT

The objective of this research is to examine users' cybersecurity behavior in monetary gain and loss scenarios. Using Prospect Theory, we hypothesize that users are more likely to engage in risky cybersecurity behavior to avoid monetary losses than to benefit from monetary gains. We also hypothesize that guaranteed gains have a greater effect on a user's risk-taking behavior than potential gains, and potential losses have a greater effect on a user's risk-taking behavior than guaranteed losses. An experimental study is proposed to test the research hypotheses.

Keywords

Cybersecurity, prospect theory, gain, loss, monetary value.

INTRODUCTION

The information security architecture of an organization is mainly dependent on the users, technology, and cybersecurity policies. Users play a crucial role as they interact with the different components of the information security architecture in an organization. A research study has found that users are the major cause for intrusions to the cybersecurity infrastructure of an organization (Sasse, Brostoff and Weirich, 2001). The study also indicates that the actions of users towards cybersecurity threats are major causes of malicious intrusions and cybersecurity attacks in organizations. The lack of cybersecurity knowledge is one of the main causes for cybersecurity threats in an organization (Chan and Mubarak, 2012). Major vulnerabilities to cybersecurity in organizations are due to the lack of awareness about information security polices, and they can lead to cybersecurity attacks such as phishing, malware, malvertising, and drive-by download.

Although security awareness among employees of an organization can be increased by making information security training mandatory to employees and explaining the information security policy to them, they do not guarantee that employees will follow the rules and guidelines in the policy. Warkentin and Willison (2009) found that personality traits and human factors could influence the perceptions of users regarding cybersecurity. Hence, more research is warranted to gain a better understanding of the human factors associated with cybersecurity threats, so that vulnerable user behavior can be minimized or avoided.

In this research, we study the behavior of users in scenarios where monetary value gains and losses are involved. We draw on Prospect Theory in the behavioral economics and decision-making literature to hypothesize and analyze user behavior in vulnerable cybersecurity scenarios.

LITERATURE REVIEW

User Behavior and Cybersecurity

Users are the weakest link in the cybersecurity chain (Sasse et al., 2001) and the most vulnerable target of cybersecurity threats (Siponen, 2000). Siponen (2000) found that end users in organizations do not follow information security guidelines, which lead to the occurrence of cybersecurity threats including phishing and other forms of attacks. A study that is based on the Protection Motivation Theory (PMT) indicates that secure behavior of users can be predicted using their self-efficacy, which refers to a belief that one possesses toward achieving or accomplishing a specific goal (LaRose, Rifon and Enbody, 2008). Factors that influence a user's cybersecurity actions include perceived severity, response cost, perceived susceptibility, and self-efficacy (Woon, Tan and Low, 2005).

In most cases, a user's willingness to adhere to the organizational security policy is not motivated by the efforts of the organization (Tyler and Blader, 2005). Although recognitions to acknowledge the desired information security behavior of users or punishments for not adhering to the rules indicated in information security policies may both serve as a form of external motivation, it is an employee's intrinsic desires that create the internal motivation to follow or not follow the policies of the organization (Tyler and Blader, 2005). Another study that is based on PMT found that users' attitude toward information security policies is influenced by two factors: threat appraisal and coping appraisal (Bulgurcu, Cavusoglu and Benbasat, 2010). Aurigemma and Panko (2010) found that the intention of a user to comply with information security policies (ISP) depends on his/her own evaluation and beliefs. They explained that the greater the notion of control the user develops over those actions, the greater is his/her intention to comply with the ISP of the organization.

Deterrence theory, which originated from psychology, explains how fear of punishment can be used to control the behavior of individuals (Gibbs, 1968). This theory is later associated with criminology to control the criminal acts of people in order to reduce crimes. Known as General Deterrence Theory (GDT) in criminology, the theory states that an individual's fear of punishment has a negative impact on the motive to commit crimes. As the importance of cybersecurity in organizations and their associated risks have been increasing, studies related to GDT in the domain of cybersecurity have also been investigated (D'Arcy et al., 2009). The GDT based research by D'Arcy et al. (2009) found that decisions made by users were largely influenced by the possible effects that users experience after making those decisions. Users think about the possible repercussions of decisions, like the perceived certainty of sanctions or the loss that they might face, which in turn influence their decisions on ISP compliance. In most of the cases, the user prefers to adopt an approach that is the easiest, requires the least training, or takes the shortest time for implementation. Such approaches often cause threats to information security. Past literature also suggests that even though users possess prior knowledge about cybersecurity threats and the necessary actions to avoid these threats, they fail to take the appropriate actions, and instead pursue cyber risks out of fear or for benefits and rewards (Lee and Kozar, 2005; Sasse et al., 2001; Stanton, Stam, Mastrangelo and Jolton, 2005).

Framing, Gains, and Losses

Studies have been carried out to evaluate the impact of positively and negatively framed messages on user behavior (Aaker and Lee, 2001; Shiv, Edell and Payne, 2004). Similarly, users make their cybersecurity choices based on potential or certain gains or losses conveyed in the message (Beebe, Young and Chang, 2014; Nah, Cheng, Smith and Ravindran, 2017; Smith, Nah, Cheng and Ravindran, 2017; Valeccha, Chen, Herath, Vishwanath, Wang and Rao, 2016). Prospect theory, which will be further discussed later, suggests that people tend to react more toward losses than gains, which is a concept known as loss aversion (Tversky and Kahneman, 1984). In addition, people prefer certainty in a gain scenario and are more willing to take risk in a loss scenario (Tversky and Kahneman, 1986). Consistent with prospect theory, research in information security has shown that people are more inclined toward taking risks when presented with a case framed as financial losses (i.e., negative framing) (Beebe et al., 2014). On the other hand, when the same problem has been framed positively, in the form of financial gains, people prefer not to take risks (Beebe et al., 2014).

THEORETICAL FOUNDATION AND HYPOTHESES

To understand cybersecurity behavior of users in scenarios involving gains and losses, we draw on the prospect theory that is based on the economic principles of decision making under uncertainty (Fishburn, 1970; Kahneman and Tversky, 1979, 1982).

The choices made by people are based on their acumen, and the acumen which people perceive is based on the relative evaluation of all the external factors of the world. Making these choices can be strenuous from a user's perspective, as it involves scenarios where the decisions endorse conflicting standards and objectives. A fundamental way to understand a rational decision-making condition is to analyze the condition or the information that is being presented to the user to form the basis of the decision. In cybersecurity related scenarios, the process of decision making is even more complex as the user's decision can be influenced by both the data or information and the way the message is framed. For example, prospect theory can be used to explain how users' decisions are assessed.

Figure 1 presents people's valuation of gains and losses according to prospect theory. Because losses are generally perceived as greater than gains, people tend to be more risk seeking to avoid losses and more risk adverse with respect to gains (Tversky and Kahneman, 1984). Hence, people are more willing to engage in risky computer security activities to avoid a loss than to receive a gain. Thus, we hypothesize that:

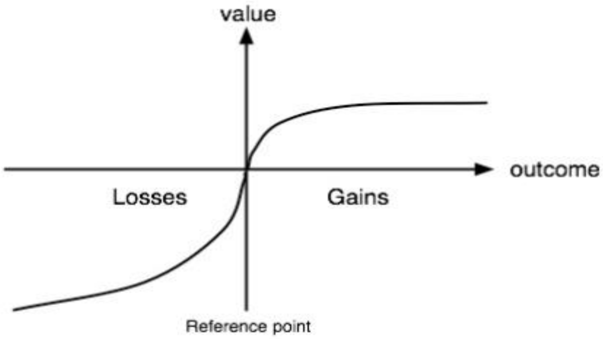

Figure 1: Prospect Theory

H1: Users are more willing to engage in risky computer security activities to avoid a loss than to receive a gain.

H1a: Users are more willing to engage in risky computer security activities to avoid a guaranteed loss than to receive a guaranteed gain.

H1b: Users are more willing to engage in risky computer security activities to avoid a potential loss than to receive a potential gain.

According to prospect theory, people are more risk seeking to avoid losses, and hence, they prefer a probable loss (i.e., an outcome associated with some uncertainty of occurrence) to a guaranteed loss when the expected loss is controlled or held constant (Tversky and Kahneman, 1984). In contrast, people are more risk adverse with respect to gains, and hence, they tend to favor a guaranteed or certain gain over a potential or probable gain when the expected gain is controlled (Tversky and Kahneman, 1984). People perceive a probable loss as an option through which they could avoid the loss as compared to a guaranteed loss. People were presented with the following conditions in an experiment where in addition to whatever they own, they were given $2000, and they are asked to choose between two choices: i) 50% probability that they lose $1000, and ii) 100% probability that they lose $500. 69% of them chose the first choice of taking the risk (i.e., 50% probability) of losing $1000 (Tversky and Kahneman, 1984). Hence, even though the expected value of both choices was similar, the way in which people perceived them was different. Interestingly, the opposite behavior was observed when presented with the guaranteed gain and probable gain conditions. Even though the expected value in both the guaranteed and probable gain conditions was the same, people demonstrated a preference for a 100% probability of a gain as compared to a 50% probability of a gain (Tversky and Kahneman, 1984). In other words, a guaranteed gain is preferred to a probable gain, and a probable loss is preferred to a guaranteed loss. Hence, we hypothesize the following:

H2: Users are more willing to engage in risky computer security activities to avoid a potential loss than a guaranteed loss.

H3: Users are more willing to engage in risky computer security activities for a guaranteed gain than a potential gain.

RESEARCH METHODOLOGY

A 2 X 2 between-subjects factorial design will be used to test the hypotheses. The first factor is value, which has two levels: gain and loss. The second factor is certainty, which has two levels: yes (guaranteed) and no (potential/probable). Hence, there are four conditions in the experimental design: (i) guaranteed gain, (ii) guaranteed loss, (iii) potential/probable gain, and (iv) potential/probable loss. This experiment will be carried out as a computer-based survey study. Subjects will be randomly assigned to one of the four experimental conditions. Each subject will be provided with cybersecurity scenarios and will be asked to make decisions on whether to download an app from an uncertified source based on the condition in each given scenario. For the (guaranteed/potential) loss condition, subjects will be told that they (will/may) incur a monetary value loss if they do not download the app. For the (guaranteed/potential) gain condition, subjects will be told that they (will/may) receive a monetary value gain if they download the app. Manipulation checks will be included to ensure that the subjects understand the condition given to them before they make their choice of action.

EXPECTED CONTRIBUTIONS AND CONCLUSION

This research study will provide a more in-depth understanding of the applicability of prospect theory for explaining and predicting user behavior in scenarios related to cybersecurity. With a better understanding of the applicability of prospect theory, we hope to be able to implement warning systems to users. In future research, we are interested in using prospect theory to assess the effects of non-monetary gain and loss scenarios on cybersecurity and compare their outcomes with scenarios that are monetary based. With a better understanding of user behavior in gain and loss contexts, email spam filters could also be optimized to detect phishing emails that offer potential or guaranteed gains or losses to entice users to download an app or software, thereby helping to eliminate or reduce cybersecurity attacks in organizations.

REFERENCES

1. Aaker, J. L. and Lee, A. Y. (2001) "I" seek pleasures and ‘we’ avoid pains: The role of self-regulatory goals in information processing and persuasion, *Journal of Consumer Research*, 28, 1, 33-49.
2. Aurigemma, S. and Panko, R. R. (2010) The detection of human spreadsheet errors by humans versus inspection (auditing) software, *Proceedings of the European Spreadsheets Risks Interest Group,* University of Greenwich, London, *73-85*.
3. 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.
4. Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 34, 3, 523-548.
5. 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.
6. D'Arcy, J. and Herath, T. (2011) A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20, 6, 643-658.
7. Fishburn, P. C. (1970) Utility theory for decision making. *Operational Research Quarterly*, 22, 308-309.
8. Gibbs, J. P. (1968) Crime, punishment and deterrence. *Southwestern Social Science Quarterly*, 48, 515-530.
9. Kahneman, D. and Tversky, A. (1979) Prospect theory: An analysis of decision under risk, *Econometrica*, 47, 2, 263-291.
10. Kahneman, D. and Tversky, A. (1982) Judgment under uncertainty: Heuristics and biases. Cambridge University Press, New York, NY.
11. LaRose, R., Rifon, N. J. and Enbody, R. (2008) Promoting personal responsibility for internet safety. *Communications of the ACM*, 51, 3, 71-76.
12. Lee, Y. and Kozar, K. A. (2005) Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, 48, 8, 72-77.
13. Nah, F., Cheng, M., Smith, S. and Ravindran, S. (2017) Impact of monetary value gains and losses on computer security behavior of users, *Proceedings of IFIP WG8.11/WG11.13 2017 Dewald Roode Workshop on Information Systems Security Research*, Tampa, Florida.
14. 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.
15. Shiv, B., Edell, J. and Payne, J. W. (2004) Does elaboration increase or decrease the effectiveness of negatively versus positively framed messages? *Journal of Consumer Research*, 31, 1, 199-208.
16. Siponen, T. M. (2000) A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8, 1, 31-41, Available at https://doi.org/10.1108/09685220010371394
17. Smith, S., Nah, F., Cheng, M. and Ravindran, S. (2017) The impact of monetary value gains and losses on cybersecurity behavior, *Proceedings of the Midwest Association for Information Systems Conference*, Springfield, Illinois.
18. Stanton, J., Mastrangelo, P. R., Stam, K. R. and Jolton, J. (2004) Behavioral information security: Two end user survey studies of motivation and security practices. *Proceedings of the Tenth Americas Conference on Information Systems*, New York.
19. Tyler, T. R. and Blader, S. L. (2005) Can businesses effectively regulate employee conduct? The antecedents of rule following in work setting, *Academy of Management Journal*, 48, 6, 1143-1158.

20. Tversky, A. and Kahneman, D. (1984) Choice, values, and frames, *American Psychologist*, 39, 4, 341-350.
21. Tversky, A. and Kahneman, D. (1986) Rational choice and the framing of decisions, *The Journal of Business*, 59, 4, 251-278
22. Valecha, R., Chen, R., Herath, T., Vishwanath, A., Wang, J. R. and Rao. H. R. (2016) Reward-based and risk-based persuasion in phishing emails, *Proceedings of the 2016 IFIP WG8.11/WG11.13 Dewald Roode Workshop on Information Systems Security Research*, Albuquerque, New Mexico.
23. Warkentin, M. and Willison, R. (2009) Behavioral and policy issues in information systems security: The insider threat, *European Journal of Information Systems*, 18, 2, 101-105.
24. Woon, I., Tan, G.-W. and Low, R. T. (2005) A protection motivation theory approach to home wireless security. *Proceedings of the 26th International Conference on Information Systems*, Las Vegas, Nevada.