Dual-process Accounts of Reasoning in User's Information System Risky Behavior

(Research in Progress)

Ying Li
Dalian University of Technology
yingli@dlut.edu.cn

Nan Zhang
University of Jyvaskyla
nan.x.zhang@jyu.fi

Abstract

End user of information system (IS) is the weakest point in terms of IS security. A variety of approaches are developed to convince end users to avoid IS risky behaviors. However, they do not always work. We would like to argue that one of the reasons is that previous studies focused on System 2 thinking (analytic, deliberate, rule-governed and effortful process) and overlooked the factors that can influence people who are using System 1 thinking (automatic, effortless, associative and intuitive process). In this study, we propose a model that integrates influential factors for both modes of thinking together. Moderators of such relationships will be discussed as well. A laboratory experiment will be conducted to verify the proposed theory. Neuroscience technique will be used to differentiate the two modes of thinking.

Keywords: Dual-process theory, system 1 thinking, system 2 thinking, IS security

1. Introduction

Information system (IS) is pervasive in people's everyday life. When people rely more and more on the convenience of such systems, the protection of data in IS becomes a central concern of both service providers and individual users. According to a recent report, IS security incidents soared 60% in healthcare in 2015. Power and utility companies detected 527% more incidents in their IS in 2014, over 2013. The average cost of a corporate data breach increased 15% in the 2015 to $3.5 million.[1] Although engineers in computer science have developed a variety of security mechanisms to maintain and enhance the IS security, end user is still the weakest point in the whole system. User's behavior often put the IS in to risk in terms of destroying the integrity, confidentiality and availability of data. In this study, we define such behavior as IS risky behavior.

To solve the problem, researchers in IS security area have identified a variety of models to explain end users' risky behavior. The theoretical foundations used by previous studies include deterrence theory (e.g., Herath and Rao 2009), rational choice theory (e.g., Bulgurcu et al. 2010), accountability theory (Vance et al. 2013, 2015), reactance and justice theories (e.g., Lowry and Moody 2015), and protection motivation theory (e.g., Herath and Rao 2009). These studies have made notable contributions to our understandings about individual's IS security behavior. However, the mixed empirical results of these studies also shown that the factors that are thought to be influential do not always work. We would like to argue that the failure is related to the assumptions they used about the mode of thinking that people may use to process risk related information. According to dual process theory, there are two different ways the brain forms

[1] https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/

thoughts: System 1, which is fast, automatic, frequent, emotional, stereotypic, and subconscious; and System 2, which is slow, effortful, infrequent, logical, calculating, and conscious (Kahneman 2011). In the research mentioned above, System 2 thinking occupies a dominant role. The fundamental assumption of these researches is that human being is rational. People can calculate benefit and cost and therefore make a best decision according to logical standards. In this case, although drawing on different theories, in general, studies in this stream try to emphasize the effects of the negative consequences of risky behavior, such as severity of a threatened event, vulnerability of the individual to an attack, and formal or informal punishment of risky behavior. In other words, studies in this stream believe that the decision of risky behavior is based on System 2 thinking. However, in reality, System 2 thinking may not be always triggered. According to Alos-Ferrer and Strack (2014), decision making involves the use of both System 1 and System 2 processes, depending on the personal characteristics and situational factors, the mode of thinking (System 1 or System 2) may differ. People may use different modes of thinking to process the same message due to different contextual factors and therefore may have different decisions. Specifically, when system 1 thinking occurs, peripheral cures that are external to the message itself affect people's decision. When system 2 thinking occurs, the quality of message arguments will be important (Petty and Cacioppo 1986). Thus factors that can influence people's decision under system 1 thinking are overlooked by previous studies. Further, contextual factors which can moderate the direct effect from peripheral cues and quality of arguments on people's decision are not controlled in previous studies.

The gaps mentioned above are hard to be solved by the traditional data collection method in behavior research, such as self-report survey. However, by facilitating neuroscience techniques, such as Magnetoencephalography (MEG), we can observe the individuals' brain activities and therefore know which mode of thinking they are using to process the information. Therefore, in this study, we will first identify the factors that may have direct effects on individual's decision in both modes of thinking. Then, we will identify moderators that can either enhance or weaken the direct effects. Finally, we will verify the model via a laboratory experiment with the help of MEG to monitor participants' brain activities.

2. Theoretical Background

Dual process theory suggests that there are two distinctively separate cognitive systems underlying thinking and reasoning. These systems are often referred to as "implicit" and "explicit" or by the more neutral terms "System 1" and "System 2" thinking. System 1thinking relies upon frugal heuristics yielding intuitive responses, while System 2 thinking relies upon deliberative analytic processing (Gervais and Norenzayan 2012). Dual process theories have been successfully applied to diverse domains and phenomena across a wide range of fields (see a review by Evans 2008)

In IS security literature, System 2 thinking occupies a dominant role (Wright et al. 2014). Persuasive techniques that are designed based on System 2 thinking provide detailed descriptions of the threats and negative consequences, and expect people to make a rational decision by a systematical evaluation of the current situation. For example, severity of a threatened event and vulnerability of the individual to an attack are supposed to influence individual's behavior decision, which are used by previous studies to encourage people to comply with the IS security policy. Recently, System 1 thinking based persuasive techniques that take advantage of an

individual's tendency to rely on automatic information processing are also introduced to IS security research. For example, research has found that unless alerted to potential harm, individuals rely on simple rules of thumb when processing phishing emails (Jingguo et al. 2012, Wright et al. 2014).

3. Theory Development

Depending on personal and situational factors, people may use either one mode of thinking to process risk related information. For each mode of thinking, the influential factors of people's IS risky behavior decision are different. Therefore, in this study, we propose a model that put the two modes of thinking in the same picture with moderators (see Figure 1).

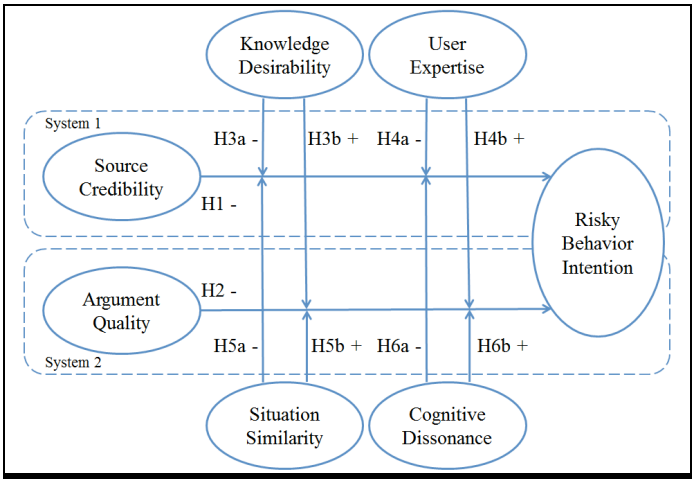

Figure 1. Research Model

3.1 Dual Process in IS Risky Behavior Decision

Previous studies suggested that people with different modes of thinking may depend on different factors to make a decision (Bhattacherjee and Sanford 2006). Specifically, two general concepts, source credibility and argument quality, are used by previous studies respectively (Petty and Cacioppo 1986). People who use system 1 thinking to process information tend to rely on peripheral cues such as source credibility to make a decision. People who use system 2 thinking to process information engage in thoughtful processing of an information message and, therefore, tend to be more persuaded by argument quality (Kahneman 2011).

In our context, source credibility is defined as the extent to which an information source is perceived to be credible by information recipients (Sussman and Siegal 2003). Further, it contains three dimensions: source expertise, source trustworthiness and source attractiveness (McCracken 1989). Source expertise refers to the extent to which information recipients perceive that an information source is competent in the domain. Source trustworthiness refers to the extent to which information recipients perceive that an information source is trustful. Source attractiveness refers to the extent to which information recipients perceive that an information source is attractive. Consistent to the previous studies, people who use system 1 thinking to process risk related information tend to rely on source credibility to make fast, automatic and subconscious decisions. Therefore, for such people, source credibility of the message will influence their risky behavior intention negatively.

H1: When people use System 1 thinking, source credibility of informational messages has a negative effect on user's risky behavior intention.

Argument quality is defined as the extent to which an argument about the risky behavior is perceived to be strong (Bhattacherjee and Sanford 2006). Specifically, previous studies suggested that the strength of the arguments on severity of a threatened event, and vulnerability of the individual to an attack can influence people's risky behavior intention. People who use system 2 thinking to process risk related information will evaluate the severity of a threatened event and vulnerability of the individual to an attack systematically and then make slow, effortful and logical decisions. Therefore, for people who are using System 2 thinking, argument quality of the message will influence their risky behavior intention negatively.

H2: When people use System 2 thinking, argument quality of informational messages has a negative effect on user's risky behavior intention.

3.2 Moderators of Dual Process

According to Stiff and Mongeau (2003), there is a variety of situational and personal characteristics that can moderate the direct link between source credibility and behavior intention, as well as the link between argument quality and behavior intention. The two most influential factors are motivation (Petty and Cacioppo, 1979) and ability (Petty et al. 1976). In additional, personal relevance and cognitive dissonance are also relevant to people's mode of thinking.

In the context of IS security behavior, motivation is operationalized as knowledge desirability and is defined as the desire to learn IS security knowledge from the message. Individuals who take greater pleasure in learning than others tend to engage in more effortful thinking because of its intrinsic enjoyment for them (Kruglanski et al. 2012).

H3a: Knowledge desirability has a negative moderating effect on the association between source credibility and risky behavior intention.
H3b: Knowledge desirability has a positive moderating effect on the association between argument quality and risky behavior intention.

Ability is operationalized as user expertise and is defined as the information recipient's capability for critical evaluation of IS threats. People who have more knowledge on information threats may tend to evaluate the argument of the message systematically.

H4a: User expertise has a negative moderating effect on the association between source credibility and risky behavior intention.
H4b: User expertise has a positive moderating effect on the association between argument quality and risky behavior intention.

Personal relevance is operationalized as situation similarity and is defined as extent to which the information recipients believes that they may engage in the same situation as described in the message. Those people who are thinking they may be threatened by the same problem as mentioned by the message would think more about the issue than those who are not.

H5a: Situation similarity has a negative moderating effect on the association between source credibility and risky behavior intention.
H5b: Situation similarity has a positive moderating effect on the association between argument quality and risky behavior intention.

Cognitive dissonance is operationalized as cognitive discrepancy and is defined as the extent to which the information delivered by the message is conflicted with recipient's existing beliefs, ideas, or values. When people are presented with new information (a message) that conflicts with existing beliefs, ideas, or values, they will be motivated to go through the argument carefully to eliminate the dissonance, in order to remain at peace with their own thoughts (Kunda 1990).

H6a: Cognitive discrepancy has a negative moderating effect on the association between source credibility and risky behavior intention.
H6b: Cognitive discrepancy has a positive moderating effect on the association between argument quality and risky behavior intention.

4. Studies

Researchers have demonstrated evidences for dual processes using neuropsychological methods (Goel et al. 2000). In general, they found that different kinds of reasoning can activate one of two different systems in the brain. Specifically, the prefrontal cortex was critical in detecting and resolving conflicts, which are associated with System 2 thinking; and the ventral medial prefrontal cortex, known to be associated with the more intuitive or heuristic responses of System 1 (Goel and Dolan 2003). In our study, we will use MEG to observe brain signals during the experiment. Its strengths consist in independence of head geometry compared to EEG, non-invasiveness, high temporal resolution as opposed to fMRI and will give participants more flexibility to complete our task on a computer. In the experiment, we will ask participants to read a scenario that is related to risky behavior and contains information about source credibility, severity and vulnerability. Then, we will ask participants to make their decision on the risky behavior. The brain signals when they are making the decision will be captured by MEG. A post survey will be conducted to measure IVs and moderators.

5. Expected Results and Contributions

Depending on the results from MEG, data will be divided into two groups, System 1 thinking vs. System 2 thinking. Source credibility will be the influential factor for people in System 1 group and argument quality will be the influential factor for people in System 2 group. Moderation effects of other factors will also be tested.

This study is expected to have several contributions on IS security behavior research. First, we develop a model to integrate influential factors for both modes of thinking together. Second, we contextualize the concept of source credibility and argument quality. Third, we identify moderators that determine the mode of thinking. Last but not least, we use neuroscience technique to differentiate the two modes of thinking empirically.

References

1. Alos-Ferrer, C., and Strack, F. 2014. "From Dual Processes to Multiple Selves: Implications for Economic Behavior," *Journal of Economic Psychology* (41), pp.1-11.
2. Bhattacherjee, A., and Sanford, C. 2006. "Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model," *MIS Quarterly* (30:4), pp.805-825.
3. 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), pp. 523-548.
4. Evans, J.S.B. 2008. "Dual-processing Accounts of Reasoning, Judgment, and Social Cognition," *Annual Review of Psychology* (59), pp. 255-278.
5. Gervais, W.M., and Norenzayan, A. 2012. "Analytic Thinking Promotes Religious Disbelief," *Science* (336:6080), pp. 493-496.
6. Goel, V., and Dolan, R.J. 2003. "Explaining Modulation of Reasoning by Belief," *Cognition* (87:1), pp. B11-B22.
7. Goel, V., Buchel, C., Frith, C., and Dolan, R.J. 2000. "Dissociation of Mechanisms Underlying Syllogistic Reasoning," *Neuroimage* (12:5), pp. 504-514.
8. Herath, T., and Rao, H. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems* (18:2), pp.106-125.
9. Jingguo W., Herath T., Rui C., Vishwanath A., and Rao, H.R. 2012. "Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email," *IEEE Transactions on Professional Communication* (55:4), pp. 345-362.
10. Kahneman, D. 2011. *Thinking, Fast and Slow*, Farrar, Straus, and Giroux, New York.
11. Kruglanski, A.W., and Stroebe, W. 2012. *Handbook of the History of Social Psychology*, Psychology Press.
12. Kunda, Z. 1990. "The Case for Motivated Reasoning," *Psychological Bulletin* (108:3), pp. 480-498.
13. Lowry, P.B., and Moody, G.D. 2015. "Proposing the Control Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal* (25:5), pp. 433-453.
14. McCracken, G. 1989. "Who is the Celebrity Endorser? Cultural Foundations of the Endorsement Process," *Journal of Consumer Research* (16:3), pp. 310-321.
15. Petty, R. E., and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," *Advances in Experimental Social Psychology* (19), pp. 124-205.
16. Stiff, J.B., and Mongeau, P.A. 2003. *Persuasive Communication*, Guilford press.
17. Sussman, S.W., and Siegal, W.S. 2003. "Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption," *Information Systems Research* (14:1), pp. 47-65.
18. Vance, A., Lowry, P.B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263-289.
19. Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M., and Marett, K. 2014. "Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research* (25:2), pp. 385-400.