Aug 10th, 12:00 AM

Beyond Rational Information Security Decisions: An Alternate View

Alaa Nehme
Mississippi State University, a.nehme@msstate.edu

Merrill Warkentin
Mississippi State University, m.warkentin@msstate.edu

Kyungmyung Jang
Mississippi State University, kj1350@msstate.edu

Sumin Kim
Mississippi State University, sk2013@msstate.edu

Beyond Rational Information Security Decisions: An Alternate View

Emergent Research Forum (ERF)

Alaa Nehme
Mississippi State University
a.nehme@msstate.edu

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Kyungmyung Jang
Mississippi State University
kj1350@msstate.edu

Sumin Kim
Mississippi State University
sk2013@msstate.edu

Abstract

Extant work has examined users' security behavior in both individual and organizational contexts by mainly applying theories that assume users' rationality. While this has enhanced our understanding of the conscious factors that underlie security behaviors, the assumption of conscious rationality bounds the theoretical lens. Addressing this limitation would facilitate expanding the knowledge ecology in the information security literature. Information security studies have started to recognize this assumption. To evaluate this milieu of disparate approaches, we conduct a preliminary literature review and identify several nonconscious factors that may shape security behaviors. In this ERF paper, we discuss herd behavior, cognitive biases, automatic cognition (also termed system 1 thinking), affect, risk homeostasis, and framing effects perception. We discuss future plans to develop a research framework that integrates the alternate nonconscious factors that may underlie security behavior, thereby providing a comprehensive alternate approach to studying behavioral information security.

Keywords

Information security behavior, bounded rationality, nonconscious, protection motivation, insider threat

Introduction

Users have proven to be a weak link in the information security chain (Warkentin and Willison 2009), and as such the behavioral aspect of information security has gained focus from IS scholars. To examine employees' (non)compliance with information security policies in the organizational context (e.g., Johnston and Warkentin 2010; Merhi and Ahluwalia 2019) and citizens' voluntary security behavior in the individual and home contexts, extant information security studies have adapted different behavioral theories from different disciplines, such as psychology, criminology, and public health (for a comprehensive review, see Moody et al. 2018). Among these theories, the most dominant ones are Protection Motivation Theory (PMT), General Deterrence Theory (GDT), and Neutralization Theory (NT). In brief, PMT suggests that individuals appraise an external threat and how to cope with it, which ultimately motivates them to take the necessary protective actions against that threat. GDT posits that the intention to commit crime or to violate organizational policies is negatively influenced by the perceived severity, certainty, and celerity of sanctions. NT posits that offenders rationalize their deviant behavior through neutralization, or rationalization, techniques (e.g., 'denial of the victim'). Other less dominant theories that have also been used by information security researchers to explain employees' security behaviors consider organizational factors such as perceived organizational injustice (e.g., Willison et al. 2018) and abusive supervision (e.g., Nehme and George 2020).

While the use of the above-mentioned theories has enhanced our understanding with respect to the underlying factors that explain or predict users' security behavior, a common attribute among them is that they all assume that users (humans) are rational in their decisions and behaviors. For instance, PMT assumes that users would deliberately and consciously appraise a given information threat and the

respective security actions prior to (not) taking these actions. Similarly, GDT assumes that organizational users consciously think about the sanctions they may experience if they violate information security policies before (not) doing so. NT assumes that employees would engage in computer abuse after they consciously rationalize their actions. The less dominant theories also hold the same underlying assumption. In sum, these theories are expectancy-value based and assume the rational-choice model; in the information security context, they lay out the conscious or rational-oriented factors that shape security behavior. Nonetheless, as recent work in psychology suggests (Stanovich 1999; Strack and Deutsch 2004), other factors which are nonrational may also shape human behavior, part of which of course is information security behavior. Nonrational, or nonconscious, factors primarily differ from the rational ones in that they are not deliberately and consciously accounted for in users' cost-benefit analysis.

Recognizing the underlying assumptions in the theories we use as IS scholars would potentially facilitate expanding our "knowledge ecology," enhance our theoretical contributions, and enhance our understanding of IS phenomena (Grover and Lyytinen 2015). To that end, we present the rationality assumption undertaken by many 'information security' studies. Our research community has begun to recognize this assumption (e.g., Dennis and Minas 2018), and information security studies, while not necessarily deliberately, have started considering nonconscious (nonrational) factors in shaping users' security behavior. The significance of studying nonconscious factors is twofold. From a theoretical perspective, this would aid in explaining security behavior. From a practical perspective, this would allow for developing more effective security training and awareness tools that especially address these nonconscious factors. In a sense, such training and awareness tools would bring the nonconscious factors to users' consciousness. Based on a preliminary literature review, we identify several of these nonconscious factors. It must be noted that our preliminary literature review is essentially an initial exploratory survey into the study of nonrational factors in the behavioral information security domain. It is not intended to be an exhaustive review but aimed at providing an initial overview of the current advancements in this matter of interest. We discuss the following nonconscious factors in the next section: herd behavior, cognitive biases, automatic cognition (also termed system 1 thinking), affect, risk homeostasis, and framing effects perception. Following this ERF, our future research plans include identifying other nonconscious factors and then developing a research framework that integrates these alternate factors, thereby providing a comprehensive alternate approach to studying behavioral information security. We hope that this would guide future information security research.

Nonconscious and Nonrational Factors

Herd Behavior

The "bounded rationality" view (Simon 1976) signals that the rationality assumption neglects that imperfect information, which leads to high perceived uncertainty, limits people's ability to engage in rational decision making. In uncertain situations, people follow the herd, often because they perceive that others know more than they do. In other words, people engage in herd behavior (i.e., when "everyone does what everyone else is doing, even when their private information suggests doing something quite different;" Banerjee 1992). Note that this can also be a rational behavior if one were to perceive high levels of personal uncertainty.

Recent information security studies (i.e., Vedadi et al. 2021; Vedadi and Warkentin 2020) have examined how users' herd behavior may contribute to their security behaviors and how users may cope with information threats. Overall, empirical evidence from these studies suggests that popularity information on the adoption of adaptive security artifacts (specifically, password managers) triggers herd behavior and can subsequently influence adaptive security behaviors (Vedadi et al. 2021). Evidence also suggests that in uncertain situations, individuals' herd mentality increases, and so do their protection-motivated behaviors following imitating others (Vedadi and Warkentin 2020). However, further investigation is warranted.

Cognitive Biases

There are at least four cognition biases related to the information security domain (Ceric and Holland 2019). The first bias is selective perception. This means that decision-makers use their perceptions, beliefs, and hypotheses to appraise information security threats. For example, if a decision maker believes that an anomaly detection is reliable, he or she may ignore solutions from others. The second bias is related to exposure to limited alternatives. For example, if information security managers do not have any experience

with information security accidents, then they would be more likely to relax their attitude toward information security updates. This bias is highly relevant for not creating alternative decisions to reduce information security risks. The third bias is related to adjustment and anchoring problems. The bias reflects not changing one's initial judgments about information security risks even when new information is available. The fourth bias is related to the illusion of control. This bias is common among decision-makers who have optimistic perceptions related to controlling security breaches. They believe that they can control any problems even when security breaches are very severe. These biases can drift a person from rationality to risky decisions. As related to theories applied in the information security domain, these biases facilitate relaxing the theory boundaries related to rationality (Chen et al. 2021). To that end, considering these cognitive biases in security context help us better understand security behavior. These and other cognitive biases should be investigated further as factors contributing to individual security decision outcomes.

Automatic Cognition (System 1 Thinking)

Automatic cognition is a brain process people engage in when reacting to stimuli factors without engaging in rational deliberate cognition (Brett and Miles 2021). Many sociology researchers have used automatic cognition to explain gender inequality, racism, and the sociology of culture. For example, automatic cognition has been applied to primary cultural frames (i.e., gender and race) that lead people to unconsciously, automatically, and near instantaneously interpret information and human behavior (Miles et al. 2019). The theoretical explanation of automatic cognition has also been also used in the information security field recently (Dennis and Minas 2018).

Dennis and Minas (2018) argue that automatic cognition is needed to predict "irrational" behavior in security breaches. To understand irrational and nonrational behavior, they suggest that personal behavior in security breaches should consider three factors: the current context, past experience, and specific stimuli.

Affect

Another discounted factor for explaining rational decision making is affect. Affect refers to the feeling of pleasure or discomfort, arousal, stress, and mood (Anderson et al. 2019). It is an umbrella term which encompasses both moods and emotions. Although these terms are used interchangeably, emotion is considered more intense and reflective of short period feelings. Mood, on the other hand, is less intense and extends for a longer period than emotions do (D'Arcy and Lowry 2019). Affect is often judged to be irrational, but it functions as an information processing mechanism with rational calculation by restricting the range of options considered, and by focusing one's attention on specific aspects of the information. Moreover, the relationship between uncertainty and affect has been well established by the previous literature (Anderson et al. 2019; Faraji-Rad and Pham 2017). Empirical evidence shows that as uncertainty increases, reliance on affect in decision making also increases (Faraji-Rad and Pham 2017). Affect is considered as a bounded rationality factor that facilitates coping with uncertainty.

The role of affect in decision making has been widely explored in different disciplines, including IS. For instance, it has been examined with respect to technology acceptance (e.g., Djamasbi et al. 2010). In information security, it has been shown that information security policy compliance is influenced by users' affective states, which vary daily (D'Arcy and Lowry 2019). Further, *affective absorption* and negative *affective flow* have been shown to lead to security policy violation decisions (Ormond et al. 2019). Further exploration of the role of affect in the context of security decisions is warranted.

Risk Homeostasis

Risk homeostasis theory proposes trade-off effects of individual safety between risk perceptions and risk acceptance levels. For example, if users are downloading illegal software, they take some risks. If illegally downloaded software is perceived to be less risky to users, then users might take more risks (i.e., sharing the illegal software). Conversely, if users' perceived risks are severe for downloading illegal software, they may reduce their exposure to such risk. In the information security domain, risk homeostasis theory is applied for information security scenarios as a valid component of information security risks (Pattinson and Anderson 2004), risk issues in information security (Farahmand et al. 2008), and antivirus software (Jardine 2020). These findings suggest that risk homeostasis theory can play a significant role in explaining

information security behavior. Many researchers assume that personal decisions from risky behaviors are bounded to rationality, but this factor's influence has not yet been empirically investigated.

However, some argue that risk homeostasis can be inevitable and automatic (Renaud and Warkentin 2017). For example, if downloading illegal software is socially unacceptable, users are not likely to admit it. Here, it is very difficult to determine the effects of risk homeostasis. To better understand the role of risk homeostasis, we need further investigation with the theoretical lens of risk homeostasis theory.

Framing Effects Perception

Framing effects mainly arise from circumstances when there are two different choices. Positive vs. negative wording of the two choices for a given problem domain is the key idea, with individuals tending to prefer positively worded choices. As outlined by extant work (Levin et al. 1998), there are three types of framing. The first type is attribute framing. This involves a given circumstance that is framed positively vs. negatively. The second type is goal framing. In this case, a convincing message is framed for communicating the positive outcomes of performing some action vs. the negative action of not performing that same action. The third is risky choice framing. Risky choice framing involves a choice between a risky and riskless option, wherein both options have an equal expected value dependent on positive or negative wording terms.

Information security studies have begun to examine framing effects (e.g., Goel et al. 2021). These effects may be used to deliver security warning messages to users more effectively. Digital nudging for the positive or negative framing of security messages is related to automatic processing of choices. Here, framing effects are an important factor for understanding automatic actions in security behavior. Prospect theory postulates that individuals are influenced more by the prospect of negative incomes than by positive ones, as embodied in the sports phrase "Losing hurts more than winning feels good." Empirical evidence suggests that framing an event as a loss will motivate more action than framing it as a gain. This principle has been applied in the security context (Goel et al 2021), but further investigation is required.

Conclusion and Future Plans

In this in-process work, we have highlighted the rationality assumption that grounds the dominant theories used by most information security studies for examining users' security behavior. We have followed by identifying and discussing several factors that facilitate relaxing this assumption. In our next steps, we plan to identify other 'nonconscious' factors, and then develop a research framework that may guide researchers' efforts in expanding our knowledge ecology as related to the explanatory and predictive factors of users' information security behavior.

REFERENCES

Anderson, E. C., Carleton, R. N., Diefenbach, M., and Han, P. K. 2019. "The Relationship between Uncertainty and Affect," *Frontiers in Psychology*, Frontiers, p. 2504.

Banerjee, A. V. 1992. "A Simple Model of Herd Behavior," *The Quarterly Journal of Economics* (107:3), MIT Press, pp. 797–817.

Brett, G., and Miles, A. 2021. "Who Thinks How? Social Patterns in Reliance on Automatic and Deliberate Cognition," *Sociological Science* (8), pp. 96–118.

Ceric, A., and Holland, P. 2019. "The Role of Cognitive Biases in Anticipating and Responding to Cyberattacks," *Information Technology & People*, Emerald Publishing Limited.

Chen, H., Turel, O., and Yuan, Y. 2021. "E-Waste Information Security Protection Motivation: The Role of Optimism Bias," *Information Technology & People*, Emerald Publishing Limited.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. *Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance*.

D'Arcy, J., and Lowry, P. B. 2019. "Cognitive-affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (29:1), pp. 43–69.

Dennis, A. R., and Minas, R. K. 2018. "Security on Autopilot: Why Current Security Theories Hijack Our Thinking and Lead Us Astray," *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* (49), ACM New York, NY, USA, pp. 15–38.

Djamasbi, S., Strong, D. M., and Dishaw, M. 2010. "Affect and Acceptance: Examining the Effects of Positive Mood on the Technology Acceptance Model," *Decision Support Systems* (48:2), Elsevier, pp. 383–394.

Farahmand, F., Atallah, M., and Konsynski, B. 2008. *Incentives and Perceptions of Information Security Risks*.

Faraji-Rad, A., and Pham, M. T. 2017. "Uncertainty Increases the Reliance on Affect in Decisions.," *Journal of Consumer Research*, Oxford University Press.

Goel, S., Williams, K. J., Huang, J., and Warkentin, M. 2021. "Can Financial Incentives Help with the Struggle for Security Policy Compliance?," *Information & Management* (58:4), Elsevier, p. 103447.

Grover, V., and Lyytinen, K. 2015. "New State of Play in Information Systems Research," *MIS Quarterly* (39:2), JSTOR, pp. 271–296.

Jardine, E. 2020. "The Case against Commercial Antivirus Software: Risk Homeostasis and Information Problems in Cybersecurity," *Risk Analysis* (40:8), Wiley Online Library, pp. 1571–1588.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), p. 549. (https://doi.org/10.2307/25750691).

Levin, I. P., Schneider, S. L., and Gaeth, G. J. 1998. "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects," *Organizational Behavior and Human Decision Processes* (76:2), Elsevier, pp. 149–188.

Merhi, M. I., and Ahluwalia, P. 2019. "Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security," *Computers in Human Behavior* (92), Elsevier, pp. 37–46.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285-A22.

Nehme, A., and George, J. 2020. "Taking It out on IT: A Mechanistic Model of Abusive Supervision and Computer Abuse," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Ormond, D., Warkentin, M., and Crossler, R. E. 2019. "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems* (20:12), p. 4.

Pattinson, M. R., and Anderson, G. 2004. "Risk Homeostasis as a Factor of Information Security.," in *AISM*, Citeseer, pp. 64–72.

Renaud, K., and Warkentin, M. 2017. "Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact," in *Proceedings of the 2017 New Security Paradigms Workshop*, pp. 57–69.

Simon, H. A. 1976. "From Substantive to Procedural Rationality," in *25 Years of Economic Theory*, Springer, pp. 65–86.

Stanovich, K. E. 1999. *Who Is Rational?: Studies of Individual Differences in Reasoning*, Psychology Press.

Strack, F., and Deutsch, R. 2004. "Reflective and Impulsive Determinants of Social Behavior," *Personality and Social Psychology Review* (8:3), Sage Publications Sage CA: Los Angeles, CA, pp. 220–247.

Vedadi, A., and Warkentin, M. 2020. "Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions," *Journal of the Association for Information Systems* (21:2), p. 3.

Vedadi, A., Warkentin, M., and Dennis, A. 2021. "Herd Behavior in Information Security Decision-Making," *Information & Management* (58:8), Elsevier, p. 103526.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), Taylor & Francis, pp. 101–105.

Willison, R., Warkentin, M., and Johnston, A. C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives," *Information Systems Journal* (28:2), pp. 266–293.