ARE WE PREDISPOSED TO BEHAVE SECURELY? INFLUENCE OF RISK DISPOSITION ON INDIVIDUAL SECURITY BEHAVIORS

Research in Progress

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

Goel, Sanjay, University at Albany (SUNY), USA, goel@albany.edu

Williams, Kevin J., University at Albany (SUNY), USA, kwilliams@albany.edu

Renaud, Karen, Abertay University, Dunee, UK, k.renaud@abertay.ac.uk

Abstract

Employees continue to be the weak link in organizational security management and efforts to improve the security of employee behaviors have not been as effective as hoped. Researchers contend that security-related decision making is primarily based on risk perception. There is also a belief that, if changed, this could improve security-related compliance. The extant research has primarily focused on applying theories that assume rational decision making e.g. protection motivation and deterrence theories. This work presumes we can influence employees towards compliance with information security policies and by means of fear appeals and threatened sanctions. However, it is now becoming clear that security-related decision making is complex and nuanced, not a simple carrot- and stick-related situation. Dispositional and situational factors interact and interplay to influence security decisions. In this paper, we present a model that positions psychological disposition of individuals in terms of risk tolerance vs. risk aversion and proposes research to explore how this factor influences security behaviors. We propose a model that acknowledges the impact of employees' individual dispositional risk propensity as well as their situational risk perceptions on security-related decisions. It is crucial to understand this decision-making phenomenon as a foundation for designing effective interventions to reduce such risk taking. We conclude by offering suggestions for further research.

Keywords: Information Security; Risk Disposition; Risk Tolerance; Risk Aversion.

1 Introduction

Are some individuals predisposed to taking security risks? This interesting question has not been answered adequately in the literature, particularly in the information security context. Research has long shown the influence of individual dispositional factors (including the so-called "Big Five Factors" and others) on a range of attitudes and behaviors. Such disposition differences might explain why two individuals with exposure to the same situations (organizational environment, training, threat vectors, etc.) often react to security threats in different ways, and why security policies do not guarantee compliance. Insiders continue to be identified as a primary vector for information security incidents (Willison and Warkentin 2013; ITRC, 2015), and why a majority of data breaches are caused by human vulnerabilities (Korolov, 2015). Such vulnerabilities enable hackers to bypass perimeter controls, such as firewalls, and enter into organizational networks or personal computers by social engineering methods, and also contribute to breaches facilitated with employees who are tricked into divulging information or permitting access to computers and networks. It is thus crucial to understand individual differences that impact employee security behavior.

It is, however, disingenuous to associate individual security behavior solely with disposition; the same individual would make dissimilar decisions in different situations. For instance, when in the middle of

a project, an employee might tend to ignore requests for software updates on computers. However, after just having finished a project, a worker would be likely to comply with a request to update software on their computer. We will approach this research by considering both dispositional and situational factors that influence security-related behavior, specifically suggesting dispositional risk tolerance or aversion as a significant factor contributing to information security behaviors. Nguyen and Kim (2017) show that there is difference in security behavior related to risk propensity; however, clearly risk propensity is highly context dependent and their research does not account for situational factors in risk-related decision making that we intend to examine. Our goal is to examine security behavior of individuals through the lens of risk decision making theories while considering both disposition and situational context.

Other researchers have studied risk-taking behavior in terms of individual differences and/or experiences. For example, Deo and Sundar (2015) demonstrated a significant gender difference in risk taking behaviors. Cameron and Shah (2015) found that personal experience of a disaster led to people behaving in a more risk averse way. Goudie *et al*. (2014) found that unhappy people were more likely to take risks than those who are happy. Even in rock climbing (Llewellyn and Sanchez, 2008), individual differences led to differences in risk-taking behavior. In several fields, there is evidence that personality differences are significantly implicated in risk-taking behaviors, and we will benefit greatly from the findings in other fields as we conduct the research outlined in this paper. Caspi *et al*. (1997) show a strong influence of personality in predicting health-risk behaviors. Mishra and Lalumière (2011) found that personality traits such as impulsivity, sensation-seeking, and low self-control were correlated with risk-taking behaviors. Jochemczyk *et al*. (2017) report that a Present-Hedonistic time perspective is linked to risk-taking propensity. Hoyle, Fejfar, and Miller (2000) found, in their study into sexual risk taking, that conscientiousness played a mitigating role in mediating risk-taking behavior.

The role of disposition and security behavior has been well studied but there is little research in the context of studying disposition and security behavior. The context of security is different than other fields where risks are relatively static compared to security where the threat landscape and risks are constantly evolving; resulting in a higher cognitive load in decision making. Also, we are evaluating users based on risk to the organization than the risk they perceive to their own wellbeing.

In this research, we plan to provide different situational contexts to users and then to elicit their projected behavior in the context. Their behavior will then be associated with their personality traits to study the role of disposition on security behavior. The rest of the paper is organized as follows: section 2 provides a brief review of the literature that focuses on the behavior theories used for explaining security behavior of individuals; section 3 presents our conceptual model for the paper along with the hypotheses and research design; section 4 discusses our methodology; section 4 discusses implications for research and practice and section 5 provides the conclusion to the paper.

2 Literature Review

Several models that capture users' rational thinking have been used to study human security behavior, including the theory of planned behavior (TPB), protection motivation theory (PMT), and deterrence theory. The *theory of planned behavior,* first proposed by Azjen (1991), suggests that the intention of an individual to engage in a behavior is directly impacted by the individuals' personal beliefs about the behavior and expectation of others towards compliance with the behavior and by the perceived control of the individual in exercising the behavior. This presumes a rational approach to decision making and action.

Protection motivation theory (PMT) (Rogers, 1983) is based on classic risk analysis that postulates that the actions of a user are driven by a "cognitive mediating process" of assessing: (1) the perceived severity of threat, (2) the perceived vulnerability to the threat, (3) perceptions of utility of recommended behavior (recommended response to the threat), and (4) the user's self-efficacy in executing the behavior. Herath and Rao (2009b) used PMT to study the security behavior of employees in organization and found that (a) threat perceptions about the severity of breaches and response perceptions of response efficacy, self-efficacy, and response costs are likely to affect attitudes toward security policy;

(b) organizational commitment and social influence have a significant impact on compliance intentions; and (c) resource availability is a significant factor in enhancing self-efficacy, which in turn, is a significant predictor of policy compliance intentions. These essential perceptions can be manipulated by communicating a fear appeal to the employee, designed to enhance threat appraisal and coping appraisal factors mentioned above (Johnston and Warkentin 2010). However, the findings from numerous PMT-based studies have been inconsistent, leading to efforts to enhance fear appeals by making them more personally relevant (Johnston, *et al*. 2015).

Deterrence theory, the other primary foundation theory for information security behavior research, is also grounded on rational choice theory, and suggests that humans base decisions on an examination of the consequences of their actions in terms of gains (pleasure) and losses (pain). By increasing the "pain" through the imposition of formal sanctions (punishment), the decision calculus is altered such that the potential offender recognizes the consequences of policy violation in the workplace (such as employment termination) and is deterred from forming the behavioral intention to engage in such transgressions. Deterrence theory holds that the individual is dissuaded by greater levels of (1) perceived sanction severity, (2) perceived sanction susceptibility (likelihood of being caught and punished), and (3) sanction celerity or swiftness. By manipulating the levels of these three factors, the theory suggests that employers can deter their employees from engaging in policy violation behaviors. In the past two decades, a number of seminal studies have applied deterrence theory to explain IS behaviors such as computer abuse (D'Arcy *et al*. 2009; Straub and Welke 1998; Harrington 1996), information security policy violations by employees (Siponen and Vance 2010; Willison and Warkentin 2011), internet usage policy violations (Ugrin *et al*. 2008), and illegal copying of software (Siponen *et al*. 2012). However, as with the application of PMT to the focal phenomenon, the research results have been mixed (D'Arcy and Herath 2011).

Each of these foundational theories is based on the assumption of rational choice in human decisions. There is an implicit assumption that we are motivated to avoid negative consequences, i.e. losses from threats or punishment via sanctions. Several studies, however, have shown that assumptions about rationality are unsound because they do not adequately explain people's actual real-world decisions. Decision makers have repeatedly been shown to violate the tenets of expected utility in making risk decisions based on framing effects (Gilovich, Friffin, and Kahneman, 2002; Hastie and Dawes 2001; Kahneman and Tversky, 1979; and Tversky and Kahneman, 1981). Tversky and Kahneman (1981) show that risk decisions are situational. Research has shown that individuals are risk-averse when dealing with gains, but are risk-seeking when faced with information regarding losses. These studies have been conducted at a population level, but we will apply these principles to our study of individual behavior. Moreover, in the information security context, people are influenced by their social context and their reliance on their colleagues (Posey *et al*., 2014).

There are likely to be individual differences that impact risk decision making. These differences need to be understood, especially in the context of information security. Warkentin *et al*. (2012a) and Johnston, *et al*. (2016) discuss the influence of personality traits and meta-traits in predicting the intention to comply with security policies and have found that complex interactions between various Big Five personality factors, known as meta-traits, influence individuals' perceptions of threats and sanctions, and offer insights into designing proper organizational measure such as security training that extends beyond the simple "one size fits all" approaches currently employed. Shropshire *et al*. (2015) evaluate the role of conscientiousness and agreeableness personality traits and found that they partially explain the discrepancy between behavioral intention and actual behavior in the security context.

Fundamentally, situational human risk behavior is likely to be influenced by individual perceptions of risk that can be simplified to an assessment of the potential *rewards* for risky behavior vs. potential *costs*. It's a balancing act: perceived rewards vs. uncertain costs. Risk taking increases as perceived magnitude of loss decreases or expected reward increases. It is clear that situational factors play a large part in decision making under uncertainty and risk. For instance, individuals may engage in high-risk behavior in their personal life yet be very conservative when making decisions at work. However, individual differences in risk tolerance and risk propensity may play a role too. That is, a person's in-

herent propensity toward risky behavior may influence the risk calculus underlying security behavior. Risk seekers are likely to have reduced perceptions of loss and reward than those who are risk-averse.

Individual risk behavior is complicated and the result of several interacting influences, including situational cues regarding rewards and threat, prior disposition to risk, possibly framed by previous outcomes in risk situations, and tendency towards sensation-seeking behaviors (Zuckerman *et al*., 1964, Zuckerman, 1974; Zuckerman and Kuhlman, 2000). Personality traits also play a role, with high risk behavior associated with high extraversion and openness, and low neuroticism, agreeableness, and conscientiousness (Nicholson *et al*., 2005).

We argue that information security behavior is influenced in part by individual differences in risk propensity. That is, a person's tendency to engage in unsecure acts is due in part to a willingness to take risks. Rohrmann (2004) defines risk propensity as a general positive attitude toward taking recognized risks. In an information security context, risk propensity may lead people to ignore or overlook security warnings and policies. In this paper, we present a blueprint of research that will examine the psychological disposition of individuals in terms of risk tolerance vs. risk aversion and the degree to which this balance will influence their security behaviors. Based on this fundamental premise, we intend to propose a model to study: (1) Impact of dispositional risk on computer security behavior; and (2) Degree to which we may be able to consequently impact risky behavior. Subsequent to this we attempt to answer the following research questions:

1. Does dispositional risk tolerance influence situational/contextual risk tolerance in context of computer security behavior?
2. Does general propensity to risk taking influence the mental calculus of risk in a specific situation, with particular application to the information security decision-making context?

3 Proposed Research Model

Our conceptual model is displayed in Figure 1 and expands on a model of decision making presented by Sitkin and Weingart (1995), which incorporated both risk propensity and risk perception (Figure 1). Risk *perception* is the assessment of "the expected loss by an individual and the uncertainty associated with the event". Risk *propensity* is defined as "an individual's tendency to undertake risky behavior" (p. 12). They further note that risk propensity is an emergent trait that evolves from outcomes of previous decisions and risk perceptions are also shaped by prior outcomes. Finally, they contend that framing can influence risk perception and consider that as an antecedent to risk perception in their model. This is a more realistic view of risk decisions and we use this to more comprehensively model security-related decision making.

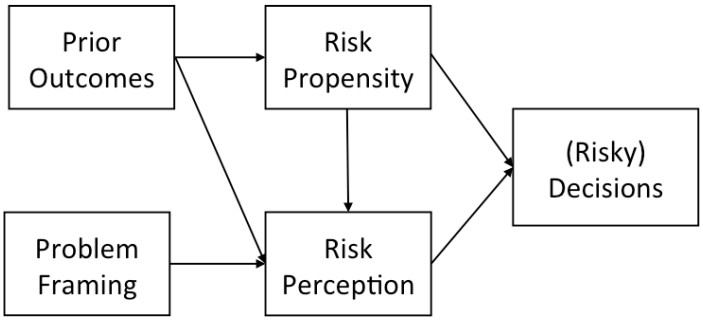

Figure 1: Sitkin and Weingart (1995) Risk Decision Model

Although risk propensity has been examined in several contexts (e.g., age (Duell *et al*., 2017), financial decision making (Stewart and Roth, 2001), gender (Morgenroth *et al*., 2017), driving behavior (Hatfield and Fernandes, 2008), health behavior (Harrison *et al*., 2005), measurement of the construct

is problematic (Renaud and Warkentin, 2017). Hatfield and Fernandes (2008) identified several problems with existing measures of risk propensity, including inferring propensity from self-reports of risky behavior (circular logic), and the failure to distinguish risk propensity from risk perception (i.e., separating the willingness to engage in risky behavior from the perception that the behavior is risky). Other research has equated risk propensity with sensation seeking, but that represents a very narrow view of what is most likely a multi-dimensional construct. Rohrmann (2004) presented and validated a multi-dimension measure of risk propensity that we will apply to the information security context. This measure assesses the motives behind valuing risk positively in addition to risk aversion and experience-seeking tendencies.

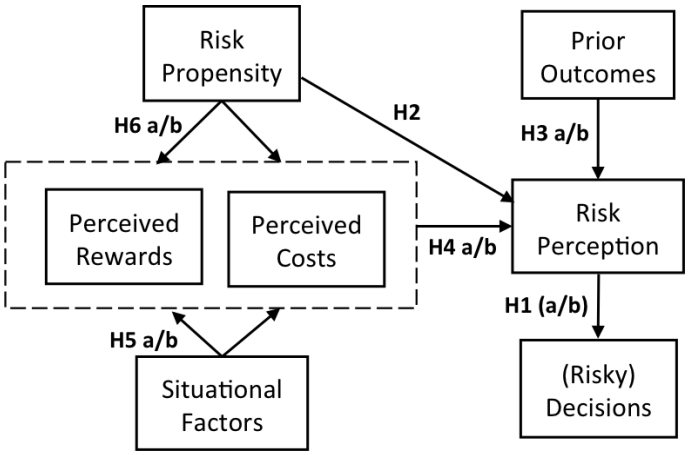

Figure 2. Conceptual Risk Decision Model

3.1 Hypotheses

Our original intention was to determine whether there was a behavioral link between risk disposition and risk perception. If such a link exists, lessened perceptions could lead to riskier behaviors. Hence we intend to explore the link between individual risk propensity and risk perception (H2), and between such perception and risk-related decisions (H1). Risk propensity is also likely to colour an individual's perception of the rewards and costs of a particular behaviour (H6), and this will potentially color their risk perceptions too (H4). Since situational factors will be likely to mediate this, we also plan to explore this causal link (H5). Finally, if they have engaged in a particular behavior before, we need to ascertain whether this impacts their risk perceptions too (H3).

$H1_a$: As perceptions of risk increase in security domain, it leads to less risky (security) behavior

$H1_b$: As perceptions of risk decrease in a security domain, it leads to more risky (security) behavior

H2: Risk propensity influences risk perception in security domain, such that individuals with high propensity for risk (or "risk-seekers") are likely to perceive less risk in any particular setting

$H3_a$: Prior positive outcomes from previous risk decisions reduces the level of risk perception

$H3_b$: Prior negative outcomes from previous risk decisions increases the level of risk perception

$H4_a$: Prior positive outcomes from previous risk decisions reduces the level of risk propensity

$H4_b$: Prior negative outcomes from previous risk decisions increases the level of risk propensity

$H5_a$: Situational factors influence perceived rewards

$H5_b$: Situational factors influence perceived costs

$H6_a$: Risk propensity influences perceived rewards

$H6_b$: Risk propensity influences perceived costs

3.2 Research Design

To assess our research hypotheses empirically, we propose an experimental design in which we measure individual dispositional variables with established scales, we manipulate situational variables (such as levels of threat and sanctions, as Johnston, *et al*. (2016) did), and we hold other variables constant, which will enable us to measure associations with (or impacts on) the dependent variable: behavioral intent either to comply with, or violate, information security policies. (We will also seek to measure actual behavior where possible, within the constraints of our data collection regime). The proximal measure for this behavior will likely be the research subject's stated security decisions within a scenario context. Furthermore, we anticipate mediation from risk perceptions – namely the perceptions of situational risk (which we will measure in the context of research scenarios) and the measure of dispositional risk by the individual decision makers, following extant rigorous measures found in the literature.

We plan to use an experimental design because our model and hypotheses are grounded in theory and published research. We are interested in testing causal relationships specified in our model and hence an experimental design is deemed most appropriate because it will allow us to manipulate independent variables, control extraneous and nuisance variables, and observe effects on outcome variables. The constructs of interest are relevant to different populations and situations and thus can be tested using various samples. We plan a combination of lab and field experiments, where we present or place participants in scenarios that require decisions to comply with security policies or heed security warnings. We will measure risk propensity as an individual variable, manipulate situational factors, measure risk perceptions, and observe decisions. We anticipate measuring prior outcomes by asking subjects about their experiences with threats and responses, using measures established by Mutchler and Warkentin (2015). We will also apply previously published and validated scales for dispositional factors such as personality traits and meta-traits (Johnston, *et al*., 2016) and dispositional risk aversion (Filbeck *et al*., 2005). The situational variables (independent variables) will be factors that might influence the cost-reward calculus that underlies security decisions, such as time urgency, workload, environmental safeguards, incentives, and social norms and pressure. All measurement scales will be developed according to established guidelines (Churchill, 1979; Diamantopoulos and Winklhofer, 2001) for scale development, including literature reviews, expert panel reviews for construct validity and face validity, and pilot studies to establish scale and item validity with confirmatory factor analysis.

Initial studies might be low-fidelity simulations where participants are presented with a number of different scenarios (that manipulate situational variables) and are asked to indicate how they would respond to the scenario. Following guidelines for mixed-method research provided by Venkatesh, Brown, and Bala (2014), we will commence with qualitative data collection using in-depth interviews to establish design validity (including descriptive validity, credibility, and transferability) and inferential validity (including interpretive validity and confirmability), which will then guide our subsequent research methods. These studies can be conducted with participants face-to-face in a laboratory setting (e.g., using university employees and students) and online with specially selected panels of participants using assessment service providers such as Qualtrics. We will follow these studies with experiments in which participants perform realistic job-related tasks that involve security decisions. We have relationships with several organizations that will allow us to recruit their employees for these experiments. We have also designed and used in-basket and job simulation tasks that can be adapted for use in these experiments.

The scenarios used in the various studies will be designed to assess the impact of disposition and situational factors (and their interaction) on a range of information security decision outcomes, such as password hygiene decisions, data backup decisions, physical security decisions, encryption decisions, online activity decisions, and others, which will enable us to generalize to information security policy compliance overall, as well as general computer security hygiene. Scenario development will conform with guidelines established by Siponen and Vance (2014).

Our model predicts that situational factors and risk propensity have indirect effects on risk perception, through perceived rewards and costs of security compliance. Risk propensity and prior outcomes are

also seen as having direct effects on risk perception. The complete model will be tested in phases. First, we will test mediated effects of situational and disposition variables on risk perception through perceived rewards and costs. We will use the bootstrapping approach to statistical mediation analysis with a categorical independent variable (i.e., situational factor) outlined by Hayes and Preacher (2014). This will allow us to assess the indirect, direct, and total effects of risk propensity and situational variables on risk perception. Next, we will test the relationship between risk perceptions and risk decisions and examine if risk perceptions mediate the effects of prior outcomes, risk propensity, and risk calculus.

4 Implications for Research and Practice

In devising interventions to reduce risk taking in the information security context, we need to ground our work in an appreciation of the variability of risk-taking behaviors leading to non-compliance. As a discipline, we do not yet have that insight. Empirical findings are required in order to advance the field in this respect. Further research is required so that we can formulate appropriate interventions that reduce risky information security behaviors. Jeffery (1989) argues that any intervention to reduce risk-taking behavior should meet three requirements: (1) benefits to the individual are substantial and virtually guaranteed, (2) the interval to realisation of the benefit is short, and (3) response cost of the behavior is low. Information security behavior, on the contrary: (1) is often costly in terms of effort, (2) benefits to the individual (as opposed to the organisation) are marginal, and (3) benefits are seldom realised at all by the person carrying out the behavior. This makes mitigation of risk taking in the security context particularly challenging. This is particularly the case if we persist in using the tried yet untested interventions currently deployed by organizational managers, namely one-size-fits-all information security training, augmented by persuasive messages (such as fear appeals) and official sanctions (punishments). We need a deeper understanding of why people decide to behave riskily, on an individual and societal level. Once we have this understanding we can design interventions in a more nuanced and effective way. In the long run, this basic scientific understanding of the nature of human decision making in this context will also convey to organizational practice as the scientific results are translated into operational programs implemented within the organizational context.

5 Conclusions and Future Work

Grounded in the perspective that individuals often follow irrational decision processes, we suggest a variance model to explain information security decisions that incorporates human dispositional factors as well as situational factors as antecedents. Deeper understanding of user decision making in the context of information security behavior will enhance our ability to tailor specific interventions for different employees to improve their effectiveness. The research is based on the human risk decision-making model proposed by Sitkin and Weingart (1995). It incorporates psychological risk propensity of individuals and their perceptions of risk based on situational factors. We seek to establish the theoretical foundations for an empirical research study to be conducted over the next year. We believe the research findings from our study will facilitate a richer, more granular application of organizational influence measures, ranging from personalized security training to customized persuasive messages, which will prove to be more effective means to encourage improved employee security decisions.

References

Ajzen, I. (1991). "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* 50(2), 179-211.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. (2010). "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* 34(3), 523-548.

Cameron, L. and M. Shah. (2015). "Risk-taking behavior in the wake of natural disasters," *Journal of Human Resources* 50(2), 484-515.

Caspi, A., D. Begg, N. Dickson, H. Harrington, J. Langley, T. E. Moffitt, and P. A. Silva. (1997). "Personality differences predict health-risk behaviors in young adulthood: evidence from a longitudinal study," *Journal of Personality and Social Psychology* 73(5), 1052-1063.

Churchill, G. A., Jr. (1979). "A paradigm for developing better measures of marketing constructs," *Journal of Marketing Research* 16, 64-73.

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville. (2013). "Future directions for behavioral information security research," *Computers & Security* 32 (1), 90-101.

D'Arcy, J., Hovav, A., and D. Galletta. (2009). "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* 20(1), 79-98.

D'Arcy, J., and T. Herath. (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.

Deo, M. and V. Sundar. (2015). "Gender difference: Investment behavior and risk taking," *SCMS Journal of Indian Management* 12(3), 74-81.

Diamantopoulos, A., and H. M. Winklhofer. (2001). "Index construction with formative indicators: An alternative to scale development," *Journal of Marketing Research* 38(2), 269-277.

Duell, N., Steinberg, L., Icenogle, G., Chein, J., Chaudhary, N., Di Giunta, L., Dodge, K.A., Fanti, K.A., Lansford, J.E., Oburu, P. and Pastorelli, C. (2017). "Age patterns in risk taking across the world," *Journal of Youth and Adolescence*, 1-21.

Filbeck, G., P. Hatfield, and P. Horvath. (2005). "Risk aversion and personality type," *The Journal of Behavioral Finance* 6(4), 170-180.

Fishbein, M., and I. Ajzen. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Gilovich, T., D. Griffin, and D. Kahneman. (2002). *Heuristics and biases: The psychology of intuitive judgment*. New York: Cambridge University Press.

Goudie, R. J., S. Mukherjee, J. E. Neve, A. J. Oswald, and S. Wu. (2014). "Happiness as a driver of risk-avoiding behaviour: Theory and an empirical study of seatbelt wearing and automobile accidents," *Economica* 81(324), 674-697.

Harrington, S. J. (1996). "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions," *MIS Quarterly* 20(3), 257-278.

Harrison, J. D., Young, J. M., Butow, P., Salkeld, G., & Solomon, M. J. (2005). "Is it worth the risk? A systematic review of instruments that measure risk propensity for use in the health setting," *Social Science & Medicine*, 60(6), 1385-1396.

Hastie, R. and R.M. Dawes. (2010). *Rational choice in an uncertain world: The psychology of judgment and decision making*. Thousands Oaks, CA: Sage.

Hatfield, J. and R. Fernandes. (2009). "The role of risk-propensity in the risky driving of younger drivers," *Accident Analysis and Prevention* 41, 25-35.

Hayes, A.F., and Preacher, K.J. (2014). Statistical mediation analysis with a multicategorical independent variable. *British Journal of Mathematical and Statistical Psychology, 67,* 451-470.

Herath, T., and H. R. Rao. (2009a). "Protection motivation and deterrence: A framework for security policy compliance in organisations," *European Journal of Information Systems* 18(2), 106-125.

Herath, T., and H. R. Rao. (2009b). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* 47(2), 154-165.

Hoyle, R. H., M. C. Fejfar, and J. D. Miller. (2000). "Personality and sexual risk taking: A quantitative review," *Journal of Personality* 68(6), 1203-1231.

ITRC. (2015). "Data Breach Insider Theft Category Summary," *Identity Theft Resource Center*, San Diego, CA, USA http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html. Accessed 23 November 2015.

Jeffery, R. W. (1989). "Risk behaviors and health: Contrasting individual and population perspectives," *American Psychologist* 44(9), 1194-1202.

Jochemczyk, Ł., Pietrzak, J., Buczkowski, R., Stolarski, M., & Markiewicz, Ł. (2017). "You only live once: Present-hedonistic time perspective predicts risk propensity," *Personality and Individual Differences* 115, 148-153.

Johnston, A. C., and M. Warkentin. (2010). "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* 34(3), 549-566.

Johnston, A. C., M. Warkentin, and M. Siponen. (2015) "An enhanced fear appeal framework: Leveraging threats to the human asset through sanctioning rhetoric." *MIS Quarterly* 39 (1), 113-134.

Johnston, A. C., M. Warkentin; M. McBride, and L. D. Carter. (2016,). "Dispositional and situational factors: Influences on information security policy violations," *European Journal of Information Systems* 25(3), 231-251.

Kahneman, D. and A. Tversky. (1979). "Prospect theory: An analysis of decision under risk," *Econometrica: Journal of the Econometric Society* 47, 263-291.

Korolov, M. (2015). "Human error is a significant factor in the majority of data breaches." *CSO Online April 10*. http://www.csoonline.com/article/2908475/security-awareness/surveys-employees-at-fault-in-majority-of-breaches.html. Accessed 22 Nov 2015.

Llewellyn, D. J., and X. Sanchez. (2008). "Individual differences and risk taking in rock climbing." *Psychology of Sport and Exercise* 9(4), 413-426.

Mishra, S., and M. L. Lalumière. (2011). "Individual differences in risk-propensity: Associations between personality and behavioral measures of risk," *Personality and Individual Differences* 50(6), 869-873.

Morgenroth, T., Fine, C., Ryan, M. K., & Genat, A. E. (2017). "Sex, drugs, and reckless driving: Are measures biased toward identifying risk-taking in men?" *Social Psychological and Personality Science*, 1948550617722833.

Mutchler, L. A. and M. Warkentin. (2015) "How direct and vicarious experience promotes security hygiene." *Proceedings of the 10th Annual Symposium on Information Assurance (ASIA)*, Albany, NY, 2-6.

Nicholson, N., E. Soane, M. Fenton-O'Creevy, and P. Willman (2005) "Personality and domain specific risk taking," *Journal of Risk Research* 8 (2), 157-176.

Nguyen, Q. & Kim, D. (2017). Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives. *Proceedings of the 2017 Hawaii International Conference on System Sciences*.

Posey, C., T. L. Roberts, P. B. Lowry, and R. T. Hightower. (2014) "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," *Information & Management* 51(5), 551-567.

Renaud, K. and M. Warkentin. (2017). Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact. *New Security Paradigms Workshop*. Santa Cruz. October.

Rogers, R. W. (1983). "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," In Cacioppo, J. T. & Petty, R. E. (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176). New York: Guildford Press.

Rohrmann, B. (2002). *Risk attitude scales: Concepts and questionnaires. Project report.* Available at http://www.rohrmannresearch.net/pdfs/rohrmann-ras-report.pdf. (Last accessed, November 25, 2015).

Shropshire, J., M. Warkentin, and S. Sharma. (2015). "Personality, attitudes, and intentions: Predicting initial adoption of information security behaviour," *Computers & Security* 49, 177-191.

Shropshire, J. D., M. Warkentin, and A. C. Johnston. (2010). "Impact of negative message framing on security adoption," *Journal of Computer Information Systems* 51(1), 41-51.

Sitkin, S. B. and L. R. Weingart. (1995). "Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity," *The Academy of Management Journal* 38(6), 1573-1592.

Siponen, M., and A. Vance. (2010). "Neutralization: New insights into the problem of employee information systems security policy violations." *MIS Quarterly* 34(3), 487-502.

Siponen, M., and A. Vance. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems* 23(3), 289-305.

Siponen, M., A. Vance, and R. Willison. (2012). "New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs," *Information & Management,* 49(7–8), 334–341.

Stewart Jr, W. H., & Roth, P. L. (2001). "Risk propensity differences between entrepreneurs and managers: A meta-analytic review," *Journal of Applied Psychology*, 86(1), 145.

Straub, D. W., and R. J. Welke. (1998). "Coping with systems risk: security planning models for management decision making," *MIS Quarterly* 22(4), 441-469.

Tversky, A. and D. Kahneman. (1981). "The framing of decisions and the psychology of choice," *Science* 211(4481), 453-458.

Willison, R. and M. Warkentin. (2012). "Beyond deterrence: An expanded view of employee computer abuse," *MIS Quarterly* 37 (1), 1-20.

Workman, M., W. H. Bommer, and D. Straub. (2008). "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* 24 (6), 2799-2816.

Ugrin, J. C., and J. M. Pearson. (2013). "The effects of sanctions and stigmas on cyberloafing," *Computers in Human Behavior* 29(3), 812-820.

Vance, A., M. Siponen, and A. Pahnila. (2012). "Motivating IS security compliance: Insights from habit and protection motivation theory." *Information & Management* 49 (3), 190-198.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly* 37(1), 21-54.

Zuckerman, M., E. A. Kolin, L. Price, and I. Zoob. (1964). "Development of a sensation-seeking scale." *Journal of Consulting Psychology* 28(6), 477-482.

Zuckerman, M. (1974). "The sensation seeking motive," *Progress in Experimental Personality Research* 7, 79-148.

Zuckerman, M., and D. M. Kuhlman. (2000) "Personality and risk-taking: Common biosocial factors," *Journal of Personality* 68(6), 999-1029.