DOES RISK DISPOSITION PLAY A ROLE IN INFLUENCING DECISIONS TO BEHAVE SECURELY?

Research in Progress

Sanjay Goel[1], Merrill Warkentin[2], Kevin Williams[1], Karen Renaud[3]
[1]University of Albany, [2]Mississippi State University, [3]University of Glasgow
goel@albany.edu, m.warkentin@msstate.edu, kwilliams@albany.edu, karen.renaud@glasgow.ac.uk

Abstract

Employees continue to be the weakest link in an organizational security ecosystem, exposing organizational assets through carelessness, malicious threats, or apathy towards security policies. Security-related decision making is a complex process that is driven by an individual's risk perception, self-efficacy, and their propensity to accept risks. Existing behavioral security research on user security behavior is rooted in models based on rational choice theory such as protection motivation theory and deterrence theory, both of which focus on using fear appeals and punishments to prompt desired security behavior. Recent research on human rationality suggests that security-related decision making is far more complex and nuanced, not a simple carrot-and-stick related process, and not necessarily grounded in rational reasoning. In reality, a combination of dispositional and situational factors is likely to interact to influence security decisions. In this paper we explore the role of one particular dispositional factor, individual risk acceptance vs. risk aversion. While not refuting the influence of other factors, we argue that this factor plays a key role in influencing security behaviors. We propose a model that depicts the impact of individual dispositional risk propensity and situational risk perception on employees' security-related decisions. We believe this model will lay a foundation for designing effective security compliance interventions.

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

1 Introduction

Employees continue to make poor cybersecurity decisions, causing security breaches and exposing organizational data (Willison & Warkentin 2013; ITRC, 2015; Korolov, 2015); it is thus crucial to understand how humans make security decisions and how we can influence the process to improve their security behavior. There is significant disparity among individuals in terms of their vulnerability to security threats, and understanding this disparity may help organizations to mitigate risks based on their employee risk profile. They may, for example, tailor training based on individual risk propensity, govern data access and set monitoring programs based on risk profile, or assign employees appropriately. Research has identified dispositional and situational risk factors. Some individuals are inherently more prone to risk-taking than others (dispositional). Other individuals take riskier decisions based on external factors (situational), such as peer pressure. Although the influence of dispositional factors on risk decisions has been studied in different contexts (see, for example, Lerner and Keltner (2000)), it has not been addressed extensively in the information security decision-making literature. Research has long shown the influence of individual dispositional factors, including the so-called "Big Five Factors" (extraversion, agreeableness, openness, conscientiousness, and neuroticism), on a range of attitudes and behaviors (McCrae and John, 1992). Such dispositional differences might explain why two individuals with exposure to the same situations (organizational environment, training, threat vectors, etc.) would react to security threats differently. In this research, we focus on investigating whether risk tolerance or aversion constitutes a significant factor contributing towards information security behaviors. Disposition, situation, and experience all play a role in influencing security decision making; our goal is to understand their relative contributions to user security decisions.

The current theoretical approaches to understanding human security behavior are grounded in rational choice models of decision making. These theories assume that people are motivated to improve gains and avoid losses (e.g. from threats of punishment). For example, *protection motivation theory* (PMT) (Rogers, 1983) is based on classic risk analysis which postulates that the user's actions are driven by a "cognitive mediating process" of assessing: (1) the perceived severity of the threat; (2) the perceived vulnerability to the threat; (3) perceptions of the utility of 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 organizations and found that (a) threat perceptions about the severity of breaches and response perceptions of response efficacy, self-efficacy, and response cost are likely to affect attitudes toward security policy; (b) organizational commitment and social influence have a significant impact on compliance intention; and (c) resource availability is a significant factor in enhancing self-efficacy, which in turn, is a significant predictor of policy compliance intention. These essential perceptions can be manipulated by communicating a fear appeal (Johnston & Warkentin 2010) to the employee, designed to enhance threat appraisal and coping appraisal factors mentioned above. However, the findings from numerous PMT-based studies have been inconsistent (Johnston *et al.* 2015).

Deterrence theory 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. 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 2013; Barlow, *et al.* 2013), 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).

Several other studies have also shown that rationality may not adequately explain 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) also show that risk decisions are situational, something these models do not incorporate. Research has shown that individuals are risk-averse when dealing with gains, but are risk-seeking when faced with information regarding losses. Moreover, in the information security context, people are influenced by their social context and their reliance on their colleagues (Posey *et al.*, 2014).

What is missing from much of the security literature is a consideration of individual differences. There are likely to be traits and dispositions that impact risk-related decision making, which should be investigated in the context of information security. Warkentin *et al.* (2012) and Johnston *et al.* (2016) discuss the influence of personality traits in predicting intention to comply with security policies, and found them to influence individuals' perceptions of threats and sanctions. 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. Such research can provide insights into designing proper organizational measures that are contextualized to different individuals in the organization.

Fundamentally, situational human risk behavior is influenced by individual perceptions of risk, which can be conceptualized as a rational (or irrational) assessment of the potential *rewards* for risky behavior vs. the potential *costs*. It is essentially a balancing act: perceived rewards vs. uncertain costs. Risk taking increases as perceived likelihood and magnitude of loss decreases or the expected reward increases. It is clear that situational factors play a large part in the assessment of risk. For instance, individuals may engage in high-risk behavior in their recreational activities (e.g., skiing), yet be very conservative when making financial decisions. However, individual differences in risk tolerance and risk propensity play a role as well. That is, a person's inherent propensity toward risky behavior may influence the risk calculus underlying risk perception and subsequent security behavior. Risk seekers are likely to have different 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, disposition to risk, and sensation-seeking behavior (Zuckerman *et al.*, 1964, Zuckerman, 1974; Zuckerman and Kuhlman, 2000). 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 well 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 study the: (1) impact of dispositional risk on computer security behavior; and (2) amount of variance in risky behavior that can be attributed to dispositional vs. situational factors.

We attempt to answer the following research questions:

1. Does dispositional risk propensity influence security-related behaviors?
2. Is the relationship between dispositional risk propensity and security behaviors mediated by situational factors?
3. Does dispositional risk propensity affect secure behaviors over and above the effects of situational factors?
4. Do prior outcomes influence risk perception?

2 Research Model

Our conceptual model extends the 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. Sitkin and Weingart's model is a more realistic view of risk decisions, and our research uses their model to more comprehensively model security-related decision making.

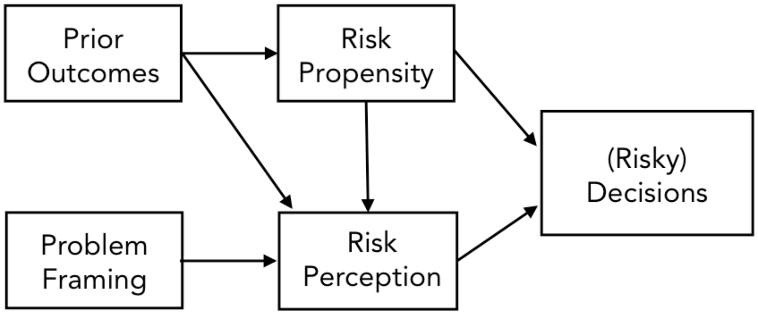

Figure 1: Sitkin and Weingart's Risk Decision Model

Although risk propensity has been examined in several contexts (e.g., financial decision making, driving behavior, health behavior), reliable measurement of the construct is problematic. 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 represents a very narrow view of what is most likely a multi-dimensional construct. Rohrmann (2004) presented and validated a multi-dimensional 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.

In our model (Figure 2), a prior outcome is considered the outcome that a person has experienced in a similar situation; situations can include, ignoring the security policy, not installing software patches, or accidentally revealing passwords. Situational factors are context-dependent factors that influence risk perception, such as a tight deadline or work pressure, which may cause an individual to ignore security policies or distribute a secure password to other co-workers. It is important to note that our model does not include all the other factors that undeniably impact risky behaviors in an information security context. This is not to suggest that they are unimportant or insignificant. Our model seeks only to test the impact of risk propensity and situational factors. A comprehensive model of decision making in an information security context would include all influential factors, and our purpose here is to determine whether risk disposition and situational factors should be included in such a model.

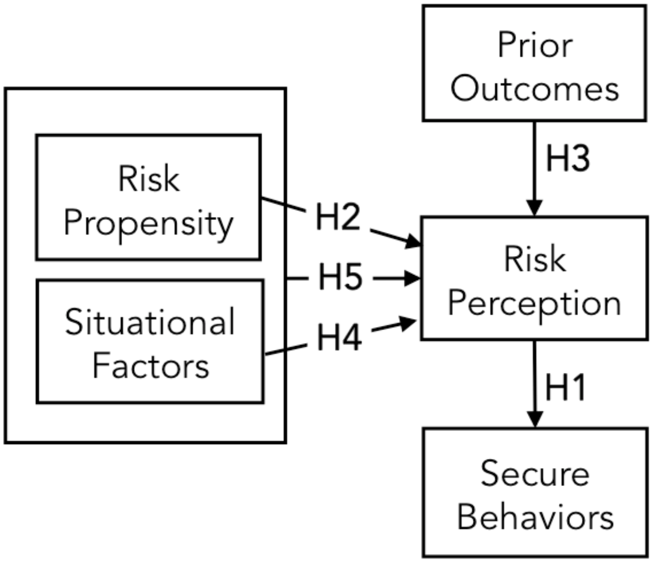

Figure 2: Conceptual Risk Decision Model

2.1 Hypotheses

The primary hypothesis is that risk perceptions are directly associated with secure behaviors.

> **H1:** As risk perception increases, so will secure behaviors.

A key component of our research is to determine the impact of risk disposition in an individual's risk perception and we articulate this hypothesis as H2, which is shown below. If a person is generally a risk taker, he/she will have a higher threshold for risky behavior resulting in riskier behavior (for instance, visiting unsafe web sites with higher chances of malware infections).

> **H2**: Risk disposition influences security risk perception, such that an individual with high propensity for risk (or "risk-seekers") is likely to perceive lower risk in any particular setting.

Prior outcomes in similar situations influence a persons' risk perception, such that if a person has engaged in prior risky behavior without negative consequences (e.g. driving at excessive speeds without experiencing an accident), their perception of risk decreases in the same or similar contexts (which could increase the chances of driving at excessive speeds). Similarly, if a person opened an email attachment that contained malware in the past, he/she will have a higher perception of risk. Hence the following hypotheses:

> **H3**: Prior (positive or negative) outcomes from previous risk decisions in similar situations impacts the level of risk perception

Situational factors also change the risk calculus of individuals, such that certain circumstances may increase or decrease tolerance of risk and risk-seeking. For instance, in a tight deadline a person would be more lax in security compared to under normal work conditions.

> **H4:** Situational factors influence levels of risk perception

Note that situational factors include fear appeals, deterrence, and other proactive managerial interventions designed to influence an individual's intention to behave in a secure manner. Johnston, *et al.* (2015) suggest that the rhetorical approach to designing such messages can be a key driver of the resulting behavioral intention. Consistent with Sitkin and Weingart (1995), Shropshire, *et al.* (2010) and Barlow, *et al.* (2013) showed that message framing can significantly influence information security behaviors.

Situational factors and risk perception may also interact with each other to inform risk perception.

> **H5:** Situational factors interact with risk propensity to influence levels of risk perception

2.2 Research Design

To empirically test our research hypotheses, we propose an experimental design in which we: 1) measure individual dispositional variables with established scales; 2) manipulate situational variables (such as levels of threat and sanctions (Johnston, et al. (2016)), and 3) hold other variables constant. This will enable us to measure associations with (or impacts on) the dependent variable, which will be compliance with information security policies. The proximal measure for this behavior will likely be the research subject's stated security decisions within a scenario context. We will also assess the kinds of security behaviors they routinely engage in, using techniques proposed by Warkentin, Straub and Malimage (2012).

For independent variables, 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). We will study situational risk assessment factors as manipulated within research scenarios.

Using a combination of lab and field experiments, subjects will complete instruments to measure their dispositional behavior traits and prior experience in risk decisions. Subsequently, they will be exposed to different situational scenarios to understand their security calculus (costs vs. rewards) and their risk perception. Subjects will also be educated on standard security guidelines during the lab session. Subsequent to the experiments, specific decision behaviors will be observed. We will assess the impacts of these dispositional and situational factors (and their interaction) on a range of information security decision outcomes, based on various scenarios similar to Johnston, *et al.* (2015), 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.

3 Implications for Research and Practice

In devising interventions to reduce risk taking in the information security context, we must ground our work on an in-depth understanding of risk-taking behaviors and consequent 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 realization of the benefit is short; and (3) the response cost of the behavior is low. Information security behavior, on the contrary is often costly in terms of effort with marginal benefits to the individual (as opposed to the organization) if any benefits are realized at all. This makes mitigation of risk taking in the security context particularly intractable, especially if we persist in 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.

4 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. A deeper understanding of user decision making in the context of information security behavior will enhance our ability to tailor specific interventions for different employees improving security compliance and effectiveness. The research is based on the human risk decision-making model proposed by Sitkin and Weingart (1995); it incorporates the 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 that will prove to be more effective in encouraging improved employee security decisions.

5 References

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

Barlow, J. B., M. Warkentin, D. Ormond, and A. R. Dennis. (2013). "Don't make excuses! Discouraging neutralization to reduce IT policy violation." *Computers & Security* 39(B), 145-159.

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.

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., A. Hovav, 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.

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.

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

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.

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.

Lerner, J. S., and Keltner, D. (2000). Beyond valence: Toward a model of emotion-specific influences on judgment and choice. *Cognition and Emotion* 14, 473-493.

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

McCrae, R. R., and John, O. P. (1992). An introduction to the five‐factor model and its applications. *Journal of Personality*, 60(2), 175-215.

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.

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.

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.

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 behavior." *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., 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.

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.

Warkentin, M., M. McBride, L. Carter, and A. C. Johnston. (2012) "Individualized security training system," *Proceedings of the National Decision Sciences Institute (DSI) Annual Conference*, November 2012, San Francisco.

Warkentin, M., Straub, D., & Malimage, K. (2012). "Featured talk: Measuring secure behavior: A research commentary," *Annual Symposium on Information Assurance & Secure Knowledge Management*, June, 5-6.

Willison, R. and M. Warkentin. (2013). "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.

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.