The Data Base for Advances in Information Systems

Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics

Nirup M. Menon
George Mason University

Mikko T. Siponen
University of Jyvaskyla

Date of Acceptance: 02/17/2019

Please cite this article as follows:
Menon, N. M., & Siponen, M. T. (Forthcoming). Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics. *The Data Base for Advances in Information Systems*, In Press.

Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics

Nirup M. Menon
George Mason University

Mikko T. Siponen
University of Jyvaskyla

Acknowledgments

We are grateful to the University of Oulu and the University of Jyvaskyla for financial support. We are also grateful to the security managers of the Finnish organizations who provided useful input for this research.

Abstract

Two aspects of decision-making on information security spending, executives' varying preferences for how proposals should be presented and the framing of the proposals, are developed. The proposed model of executives' commitment to information security is an interaction model (in addition to the cost of a security solution, and the risk and the potential loss of a security threat) consisting of the interaction between an executive's preferred subordinate influence approach (PSIA), rational or inspirational, and the framing, positive or negative, of a security proposal. The interaction of these two constructs affects the executive's commitment to an information security proposal. The model is tested using a scenario-based experiment that elicited responses from business executives across 100+ organizations. Results show that the interaction of the negative framing of a proposal and the inspirational PSIA of an executive affects his or her commitment to information security. Further, negative framing of a proposal and the cost of the security solution interact to decrease the executive's commitment to information security. This study underscores that prescriptions for business executives from normative models in information security spending must be complemented with appropriately framed messages to account for the differences in executives' PSIA (rational and inspirational) and cognitive biases.

Keywords: Resource Allocation; Negative Framing; Prospect Theory; Cognitive Bias; Heuristic Systematic Model.

Introduction

Over the years, the ubiquity of information systems and global networks has increased the potential threats to information security. Preventing and protecting against such threats has been challenging, as evidenced by the 4,200+ data breaches reported to the public and the exposure of more than 863 million records of various types to unauthorized persons since 2005.[1] Each of the breaches in 2014 at Target, Home Depot, and the U.S. Office of Personnel Management exposed millions of customers' and employees' records to unauthorized persons. Industry surveys on allocating resources for information security fault organizations and their managers for not spending enough to keep pace with the growing security threats (PricewaterhouseCoopers 2004, 2013).

Resource allocation decisions for information security differ from typical resource allocation decisions in organizations because information security is neither revenue-generating nor cost-reducing (Baskerville 1991). Many resource allocation decisions target revenue enhancement or cost reduction, and are based on—in addition to risk and cost considerations—the gains expected from the investment. Resource allocation decisions in information security are primarily based on preventing loss, and the best outcome is that "nothing happens." Inadequate resource allocation in information security in an organization may be due to an ineffective security manager or a recalcitrant executive not allocating the resources sought by a security manager (Dutta & McCrohan 2002, Gordon & Loeb 2002, Wang et al. 2008). Because business executives are the ultimate decision makers in resource allocation, this study addresses an executive's disposition toward allocating resources for information security.

An executive allocates resources for information security based on security managers' proposals and plays an important role in the information security culture of the organization (Hu et al. 2012). Several normative models in risk management and information security have been developed for resource allocation proposals (Gordon & Loeb 2002, Wang et al. 2008). Although normative models provide a quantitative basis that managers can understand and use to weigh costs and benefits, these models do not predict how a proposal's framing and executives' preference for how proposals should be presented affect decisions. Behavioral considerations such as human cognition and the executive's cognitive biases must be incorporated to better understand how predictive normative models are of real-world phenomena.

Previous research on cognition and resource allocation by executives has found preferences for broad situational information and for detailed quantitative information when executives make decisions (Chenhall & Morris 1991, Henderson and Nutt 1980, Volkema & Gorman 1998). This stream of research fashioned cognitive style as a concept that captures differences in the way individuals gather and process data. Cognitive style, however, does not capture the notion that a subordinate presents data in a specific fashion to a manager to influence him or her. A proposal presented to an executive using an influence approach that does not suit him or her is not likely to lead to the presenter's desired outcome for the proposal. In information security, managerial preferences for proposals vary, with some executives preferring proposals that are quantitative, and derived from normative models of risk management. Others prefer proposals with qualitative and inspiring rationales to persuade the executives to invest in information security. Information security practitioners argue that when an executive who prefers quantitative proposals is presented with a qualitative proposal, or vice versa, the proposal does not get funded

(Brandel 2012, Duffy 2002, Masters 2012). The concept of cognitive style does not capture the richness associated with decision making involving the proposer's approach and the decision-maker's preferred approach.

This paper proposes that a new construct, an executive's preferred subordinate influence approach (PSIA), plays a critical behavioral role in information security commitment. This construct encapsulates an executive's preference for the approach that a subordinate should use to persuade the executive to invest in a security proposal, thus highlighting the role of the executive in information security (Hu et al. 2012). The measurement of this construct is different from the measurement used for the cognitive style of an executive, because of the measurement issues associated with cognitive style (see Michael 2003 for a critique of using the Myers–Briggs Type Indicator scale to measure managers' cognitive style). Instead, a scale from the leadership literature (Yukl et al. 2008) is used to measure the types of influence approaches used by subordinates. Rather than asking subordinates what influence approaches they would use to influence an executive, the executives in the sample were polled about how they prefer to be influenced, thus capturing the preferences for quantitative versus qualitative proposals among executives.

Although the PSIA accounts for the congruence between a proposal and an executive's preferred style for the presentation of a proposal, this construct does not account for cognitive biases during decision making. As in the context of employee compliance with security policies, cognitive biases play a role in information security behaviors (Anderson & Agarwal 2010). Cognitive biases arise due to heuristic processing, which refers to cue-based, rapid decision-making. Framing of the choices in a decision context, when used by a decision maker as the primary cue, can result in biased decisions (Taylor 1991, Meyers-Levy & Maheswaran 2004). An executive must often choose between proposals differing in verbiage (i.e., framing) and content (such as risk and cost); superficial use of the differences between these cues can affect cognitive processes, decision making, and decisions. In information security, subordinates can frame a proposal positively (e.g., action increases protection) or negatively (e.g., inaction increases risk). The framing of information security proposals affects the motivation of the message recipient to exert effort in decision making. This, in turn, affects the recipient's decision, because the proposal framing—by itself, or as part of a limited number of superficial cues—is used by the decision maker to arrive at a decision (Anderson & Agarwal 2010, Johnston & Warkentin 2010).

The PSIA and framing relate to human cognition, because the former reflects a preference for how information is presented, and the latter reflects the biases that emerge due to the structure of the presentation. Thus, an overarching framework called the heuristic systematic model (HSM) is used to explain and derive a model of interaction between the PSIA and framing. According to the HSM, human cognition employs two types of processing: Heuristic processing, also called the peripheral route, is associated with cue-based rapid decision-making; systematic processing, also called the central route, is effortful and cognitively elaborates arguments (Cacioppo et al. 1986, Chaiken 1980, Duetsch & Strack 2006, Epstein 1998, Evans 2003, Kahnemann 2011, Sloman 1996, Smith & DeCoster 2000, Stanovich & West 2000). The HSM forms the basis for the logic for why the framing of an information security proposal interacts with executives' PSIA, and with the characteristics of the proposal itself, to result in differing outcomes from otherwise similar proposals. The study design followed a scenario-based experiment in which key variables were manipulated as scenarios to mimic different types of proposals. This instrument was then used to collect data from senior executives in Finland, and the data were analyzed using the hierarchical linear modeling technique to test the research model.

Literature Review

In this section, the literature on allocating resources for information security, the HSM and framing, and executives' PSIA, is reviewed.

Allocation of Resources for Information Security

An explanation that is given for why information gets compromised at the hands of hackers is that information security is a weak-link phenomenon; all a wrongdoer needs to do is to find the "weakest link" to gain access to information (Anderson & Moore 2006). The information security literature identifies the end user as a weak link (Johnston & Warkentin 2010). Another weak link is inadequate resource allocation for information security by executives (Dutta & McCrohan 2002, Magnusson et al. 2007). Resource allocation for information security is regarded as inadequate from two perspectives. First, information security managers claim that senior executives do not allocate resources to information security to the extent that security managers consider necessary (Magnusson et al. 2007). Second, as a percentage of information systems spending, information security resources are inadequate. An industry survey claims that although information security investments have been increasing in recent years, information security threats and risks have increased even more

(PricewaterhouseCoopers 2004, 2013). As a result, despite the increases in information security investments, companies could remain underinvested in information security.

Organizations have limited resources, and information security investments compete with other investments that have high revenue potential (Magnusson et al. 2007). Information security investments do not directly increase revenue, and their impact on preventing financial losses is difficult to show (Baskerville 1991). Managerial decisions about resource allocation for information security rely on the potential loss from a breach, the risk of a breach, and the cost of the proposed solutions (Gordon & Loeb 2002, Puhkainen 2006). A security breach could lead to a monetary loss in the form of crashed servers, productivity disruptions, stolen credentials, and liabilities (Siponen & Vance 2010).

Among normative approaches to information security spending, it was found that a typical organization's optimal spending on information security is about 37% of the expected loss resulting from all security breaches (Gordon & Loeb 2002). Later models finessed this prescription by relaxing some of the simplifying assumptions of the original Gordon–Loeb model (Gordon & Loeb 2006, Huang et al. 2008). For example, Huang et al. (2008) relaxed the assumption that executives are risk-neutral and modeled risk aversion to normatively demonstrate that a risk-averse decision-maker continues to spend on information security until the investment is close to the potential loss amount.

Heuristic Systematic Processing

There is broad consensus that individuals deviate from normative rational decision-making, and that heuristic cognitive processing leads to biases in decision-making. For example, an individual evaluates expected losses and expected gains differently, unlike the assumption rooted in rational utility-based logic (Tversky & Kahnemann 1991). Heuristic processing is associated with contextual cues, first impressions, and cognitive miserliness, whereas systematic processing reflects decision-making associated with rationality, deliberation, and cognitive effort. Because of this difference, not all decisions that are made by an individual can be attributed to rational decision-making. Neither approach is necessarily superior in all contexts. Further, the two routes are not mutually exclusive, because 1) both cognitive processing routes are simultaneously active at varying intensities (Chaiken & Maheswaran 1994), and 2) the two routes interact with each other so that systematic processing is affected by heuristic processing and vice versa (Deutsch & Strack 2006). Typically, heuristic processing is activated first, after which systematic processing may or may not be activated (Chaiken 1980).

Framing

A primary abstraction that researchers use to analyze individuals' decision-making is the decision frame. A decision frame consists of the formulation of the problem and a decision-maker's personal characteristics (Kahneman & Tversky 1979, Tversky & Kahnemann 1981 p. 453). Experimental studies in subject areas such as psychology, health communications, marketing, and information security have operationalized framing as a semantic manipulation of an identical problem. In particular, the decision frame has been conceptualized in terms of positive and negative framing of a message (Anderson & Agarwal 2010, Block & Keller 1995, Grewal et al. 1994, Miller & Fagley 1991, Rothman et al. 1993). The difference in the decisions made by an individual when a choice is framed as an opportunity and when a choice is framed as a threat is explained by different types of utility functions (Kahnemann & Tversky 1979, Kanouse & Hanson 1972). Field studies showed that even professional financial investors exhibit this decision-making bias (Statman et al. 2006).

When presenting an information security proposal, an IS manager can choose to use either a positive or negative tone (Brandel 2012, Duffy 2002, Masters 2012). When using a positive tone, they may highlight the advantages of applying a security measure by underscoring that the organization will be better off. This option acknowledges the inherent uncertainty in the efficacy of the information security solutions and highlights that the probability of a security breach will be reduced, but not eliminated, by implementing such a solution (Anderson & Agarwal 2010). A negative tone, in contrast, highlights the negative outcomes of not implementing a security solution. For example, the IS manager points out that his or her organization will be among those that do not implement the solution, and when other companies implement a security solution to tackle the current information security problem, malcontents and unethical hackers will focus their attacks on vulnerable companies (Anderson & Moore 2006). Thus, if an IS manager tells a business manager that "we will be worse off if we do not implement the solution," this is not a false statement. The IS manager simply chose a more fatalistic tone in the negative frame in lieu of a status quo statement that maintains that the organization simply remains as vulnerable as before (Johnston & Warkentin 2010).

The findings of the effects of positive and negative framing of information security policies on employee compliance with these policies are mixed. Although some studies demonstrated that framing matters, other studies showed opposite results (Anderson & Agarwal 2010, Stanton et al. 2005, Vroom & Von Solms 2004). Some of these contradictory results have been explored in research examining the interaction of framing with manipulations such as self-efficacy, self-view, etc. (Anderson & Agarwal 2010, Fagley & Miller 1990). This paper provides a new perspective for this stream of research by focusing on heuristic and systematic processing as an underlying mechanism for the interaction among framing, an executive's PSIA, and the characteristics of an information security proposal for allocating resources.

Rational and Inspirational PSIA

When a senior executive prefers numbers and quantitative approaches during decision-making, and indicates to subordinates they should use such an approach to propose projects and solutions, this individual has a high rational PSIA. This preference is characterized by logical arguments, factual evidence, and numbers. A rational PSIA is reflected through a high need to formalize and model contextual data and information coherently (Cacioppo & Petty 1982, Simon et al. 2004). This executive will expect to be presented with the merits and demerits of a proposal, and will be generally known to others as someone who pores over numbers and logical arguments. Upon receiving a quantitative information security proposal, such an individual will employ systematic cognitive processing because the situation demands it, and the individual is inclined to a high need for cognition (Cacioppo & Petty 1982, Simon et al. 2004).

An executive who relies less on analytical decision-making and quantitative approaches and relies more on inspiring subordinates and making connections to the organization's ideals and values exhibits an inspirational PSIA (Yukl et al. 2008). A subordinate reporting to this executive would communicate proposals to arouse enthusiasm by appealing to managerial and organizational values, ideals, and inspirations (Kipnis & Schmidt 1988).[2] This executive is known to others to expect to be inspired and to be emotionally connected to the proposal (Yukl et al. 2008). The underlying cognitive processing of an inspirational PSIA is the use of heuristic processing, as in searching for cues to inspire and connect emotionally. We do not posit that rational and inspirational PSIAs are mutually exclusive in executives but that each executive possesses a higher level of one approach compared to the other. We also posit that a rational PSIA is associated with less heuristic processing compared to an inspirational PSIA.

The role of senior executives in information security is indisputable. Security culture is important, and executives play a role in shaping this culture (Hu et al. 2012). However, the question of how and why an executive would engage in information security remains unanswered. Not all individuals react to negative and positive framing in the same way (Fagley & Miller 1990, 1997). A personality's congruence with the framing of a problem can affect the decisions made by the individual (Mahoney et al. 2011). Unfortunately, there is a lack of consistent results for interactions between personality and framing (Mahoney et al. 2011, Shiloh et al. 2002, Smith & Levin 1996). Executives are not the same, and individual differences affect decision making (Fagley & Miller 1990, Stanovich & West 2000).

The PSIA is relevant for allocating resources for information security for the following reasons: 1) Perceptive subordinates are likely to use the influence tactics that an executive prefers, which makes the PSIA relevant in the organizational context, 2) the role of the PSIA in decision-making bias has not been studied thus far, 3) this approach is relevant to the problem of inadequate investment in information security, 4) the PSIA is logically linked to the cognitive perspective in that some PSIAs are conducive to influence by framing, and 5) differences in decision-making are attributable to differences in preferences for rational decision-making (Chenhall & Morris 1991, Stumpf & Dunbar 1991, Volkema & Gorman 1998).

Influence tactics have been conceptualized and observed from the perspective of subordinates trying to persuade a senior manager regarding a policy, decision, or proposal (Yukl et al. 2008). The leadership literature lists the following tactics that subordinates use to persuade their superiors: pressure, upward appeal, legitimating, exchange, coalition, ingratiating, rational persuasion, inspiration, personal appeals, and consultation (Kipnis et al. 1980, Yukl & Falbe 1990, Yukl & Tracey 1992, Yukl et al. 2008). This literature is silent about which of these tactics are favored by the subordinates' superiors, and how the superiors' preferences for different types might affect proposal outcomes. Perceptive subordinates use tactics that are favored by their superiors, and are likely to tailor their proposal using one type of tactic for one superior and another tactic for a different superior. Doing so increases the subordinate's chance of persuading his or her superior to commit to the proposal. This logic supports the concept of the PSIA, which describes what an executive prefers about a proposal when being persuaded to make a decision about it.

Hypotheses

The model proposed, shown in Figure 1, brings together the PSIA, framing, characteristics of a security problem, and an executive's commitment to information security. The logic of the interaction effect between framing and other antecedents of the commitment to information security is based on the premise that negative framing has a more dramatic effect for people who are emotional when they make a decision and a less dramatic effect for people who are rational. The starting points for the arguments for the model, following the discussion in the literature review section, are as follows. First, most individuals tend to adopt heuristic processing rather than systematic processing due to cognitive miserliness (Toplak et al. 2011). Second, a rational PSIA is positively associated with systematic processing, and an inspirational PSIA is positively associated with heuristic processing. However, a direct effect of the PSIA on commitment to information security is not assumed or hypothesized, because there is no prior literature or abstraction that relates cognitive processing to commitment to information security. Nonetheless, rational and inspirational PSIA's direct effects are retained as control variables for completeness as shown in the figure. Third, all individuals are affected by framing by varying degrees, and negative framing is likely to incite effort and systematic processing in individuals. The effect of the framing of a proposal on the commitment to information security depends on the message, the context, and the executive's PSIA, thus making it necessary to hypothesize interaction effects. No assumption is made about the direct effect of framing by itself on the commitment to information security.

INSERT FIGURE 1 ABOUT HERE

Interaction between Framing and the PSIA

A rational PSIA is a predisposition to systematic cognitive processing during decision making. A high rational PSIA is associated with a high motivation to question assumptions and analyses of the quantities presented in the proposal. A positive frame does not affect cognitive processing significantly, and thus, an executive with a rational PSIA primarily uses systematic processing. When this executive is presented with a negatively framed proposal, the negative framing incites further motivation to question the assumptions and analyses presented in the proposal; thus, more cognitive effort is exerted. Although the degree of systematic processing could arguably differ across positive and negative framing, because a rational PSIA is associated with systematic processing, this executive's commitment to information security, for a given cost, risk, and potential loss, is not likely to be affected by negative framing. Thus, we propose the following null hypothesis:

H1 (null): *The relationship between an executive's rational PSIA and commitment to a quantitative information security proposal is the same for a negatively framed proposal as for a positively framed proposal.*

An inspirational PSIA is a predisposition to heuristic processing during decision making. This means that superficial cues in the proposal will register immediately for an executive with a high inspirational PSIA. For example, deciding to reject a proposal based simply on the context, such as information security, would be a decision made based on a superficial cue. But when an executive with a high inspirational PSIA is presented with a negatively framed proposal, the negative framing provides impetus to the individual to become motivated to question the assumptions and analyses presented in the proposal (Chaiken & Maheswaran 1994, Levin et al. 2002). Negative framing of a security proposal can lead an individual to switch from registering only superficial cues to registering the details of the proposal. Systematic processing is triggered as the individual has the motivation and the ability to engage in message processing, and to study the details of the proposal. A manager's motivation to seek and process facts increases when the framing is negative. There is argumentation with oneself leading to a reduction in the impact of superficial cues (Cox & Cox 2001, Rothman & Salovey 1997). Essentially, the motivation and involvement ensuing from the negative framing cancel out heuristic processing in favor of systematic processing. If the same proposal were cast in a positive frame, the primary cognitive processing would have been heuristic. To test these arguments, we propose the following hypothesis:

H2: *The relationship between an executive's inspirational PSIA and commitment to a quantitative information security proposal is more positive for a negatively framed proposal than for a positively framed proposal.*

Cost of a Solution and the Framing of the Proposal

Most executives are not technology executives, and do not possess significant information security knowledge. Yet they must often make quick decisions about information security spending, with other business decisions

vying for their attention. An executive must rely on the quantifiable cost implications of a security solution to decide whether spending on the solution is warranted. From a rational perspective, as the cost increases, with everything else held constant, an executive is less inclined to invest in information security (Gordon & Loeb 2002). However, cost carries a negative connotation, because the term communicates a loss of current funds rather than a gain (Thaler 1990). An individual may use this negative connotation as a cue to make a decision, as explained above regarding heuristic processing (Evans 2003, 2011, Hodgkinson & Healey 2011). When a proposal is framed positively, the negative connotation is used as a cue by an individual, in addition to the information security context as a cue. The decision, based on heuristic processing, does not rely as much on the cost as a quantity but on the cost as a cue.

When a proposal is framed negatively, the individual is motivated to consider the proposal in detail and to exert effort. Using systematic processing, the individual considers the cost a quantity, rather than a cue only. In information security proposals, the cost is typically an estimate, which can vary from one individual to another. During systematic processing, the estimate of the cost provided in the proposal is questioned. The result is that the reluctance to spend on information security due to higher cost is enhanced when faced with a negatively framed proposal, all else remaining constant. Therefore, we propose the following:

H3: *The relationship between the cost of an information security solution and commitment to a quantitative information security proposal is more negative for a negatively framed proposal than for a positively framed proposal.*

Potential Loss from an Information Security Breach and the Framing of a Proposal

When learning that the potential loss from a security breach is high, an executive is likely to allocate funds to secure the systems, because individuals eschew loss, and executives are more concerned about potential losses than potential gains (March & Shapira 1987). An increase in the potential loss leads to an increase in the executive's willingness to spend on information security. Similar to the cost of a security solution, a potential loss carries a negative connotation that could be a cue that an individual picks up, as is done during heuristic processing. When an information security proposal is framed negatively, the individual's motivation and cognitive effort increase, as in systematic processing. The potential for loss no longer registers as a superficial cue; the quantity or degree of loss is considered, and the credibility of the estimate is analyzed. Because potential loss is something that is realized in the future, unlike cost (which is immediate), the credibility of the potential loss is not a serious issue for an executive. With all else constant, an increase in potential loss in a negatively framed proposal will lead to the executive committing to the proposal. Thus, the following hypothesis is proposed:

H4: *The relationship between the potential loss from a breach and commitment to a quantitative information security proposal is more positive for a negatively framed proposal than for a positively framed proposal.*

Risk of an IS Breach and the Framing of a Proposal

As the risk of an information breach increases, an executive is more likely to invest in security (Gordon and Loeb 2002). Similar to cost and potential loss, the risk of a breach carries a negative connotation. When faced with a positively framed proposal, an individual focuses on the cue that the proposal is about information security, and that an estimate of the risk is provided in the proposal. The estimate of the risk is not given much consideration; thus, managerial commitment to spend on security measures is not affected by the increasing risk, all else constant. However, when a proposal is framed negatively, the individual is motivated to exert a cognitive effort to analyze the proposed estimate of risk. As with potential loss, risk is less tangible than cost; therefore, the credibility of the estimates of the risk is not questioned. Thus, an executive's willingness to commit to security increases with the increasing risk of a breach and negative framing of the proposal, all else constant. The following hypothesis was tested:

H5: *The relationship between perceived risk of an IS breach and commitment to a quantitative information security proposal is more positive for a negatively framed proposal than for a positively framed proposal.*

Scenario-Based Experiment Design[3] and Empirical Analysis

It is difficult to obtain a large sample of field data on information security proposals, communications between IS and senior executives, and the outcomes of such proposals. Therefore, we resorted to a scenario-based experiment research design for senior executives by presenting them with hypothetical scenarios (D'Arcy et al. 2009, Jasso 2006). The focus of this study was not the outcome for an organization—in which case, we would

require data from all executives comprising the board. Instead, we are concerned with an executive's predisposition to an information security proposal and accordingly, designed the scenarios and a survey to collect data from one executive per organization.

Scenario-Based Experiment Design

Before designing the scenarios for the instrument, we brainstormed with eight experienced information security managers.[4] All had more than 15 years of experience in making security investment proposals to executives at various companies. Two had been information security consultants who were involved in preparing a number of security investment proposals for various organizations. According to these experts, an information security investment proposal is written as a *PowerPoint* style proposal, and a board member or an invited expert presents the proposal to the board. We created hypothetical scenarios in which key information was bulleted (e.g., see in Armacost et al. 1991). Such hypothetical scenarios serve as abstractions of a security proposal, as has been done in previous work on information security (D'Arcy et al. 2009, Harrington 1996, Siponen & Vance 2010).

Another design issue is the appropriate level of contextual specificity. Of the two types of measures, generic and specific (Siponen & Vance 2014), we set up the information security issue as generic rather than specific because we would have had to refer to specific technologies, such as a firewall security solution. The team of consulting practitioners noted that a particular type of investment is not only irrelevant for senior-level respondents but also underscores technicalities that an executive hardly understands, and thus, is likely to lead to incomplete and biased data. A similar issue was mentioned in the practitioners' information security survey conducted by the Ponemon Institute (2014): "executives view cyber threat information as being too technical and domain-specific for their use." Thus, we designed the experiment and hypothetical scenarios without mentioning technical issues.

We operationalized the variables *Risk of a Breach* and *Potential Loss from a Breach* as three-level categorical variables, where the levels were low, medium, and high. *Cost* was operationalized as the cost of the information security solution, ranging from 15% to 95% business value loss in 10% increments. With nine levels, the variable *Cost of a Solution* could be thought of as continuous. An example of a high-cost incident is the breach at Target, which exposed millions of credit card numbers to hackers (Bloomberg Businessweek 2014). A low-cost incident could be a simple misuse of data access privileges. Finally, the variable *Framing* was binary. A positive frame was the statement that investing in a security solution would make the organization less vulnerable to the specified threat, whereas a negative frame stated that not investing would make the organization more vulnerable.

A typical narrative in the final instrument is provided in the left-hand column of Table 1A and 1C; the right-hand column illustrates the concept being measured. We adapted seven questions or indicators from Yukl et al.'s (2008) leadership scale to measure the respondents' PSIA. We chose three indicators that corresponded to a rational PSIA, and the two corresponded to an inspirational PSIA.[5] The value for each bulleted item for a scenario in Table 1A was randomly selected. We followed each scenario with two questions or indicators to measure the latent dependent variable *Commitment* (see the question listed in the Commitment Statement in Table 1B). The first indicator is *Support,* and the second is *PosDecision*. Because the two items are likely to be highly correlated, we did not see the need for a third item to simply measure the psychometric properties of this latent variable (Gefen et al. 2011). Adding a third item that was very similar to the other two would have likely aggravated the respondents and increased the possibility of incomplete surveys.

To tease out the existence and effect of framing in general, we used five hypothetical scenarios for each individual, randomly changing the cost, risk, loss, and framing for each scenario. The total number of scenarios, based on the levels of the four variables, was large, $9 \times 3 \times 3 \times 2 = 162$. It is not likely that an executive would have answered more than five scenarios, and experiments featuring 162 scenarios are impractical for an individual to complete. Furthermore, respondent fatigue was likely to set in for each new scenario a respondent was shown. Therefore, we randomly picked five scenarios from the full set of 162 possible scenarios for each respondent. An advantage of randomly selecting the five scenarios from the full set is that the treatments could be thought of as random variables and could be entered into a regression model as independent variables (Jasso 2006). Each scenario was presented on a separate page from the other scenarios. We also randomized the order of the scenarios, as well as the bulleted information in the scenarios.

Before the scenarios and questions were finalized, the instrument was pre-tested with nine doctoral students and post-doctoral researchers. After these students completed the experiment and the survey, we discussed the conceptual model with them, asking them to react to the ability of the research design to generate reasonable measurement and variance to test the model. The survey questions were modified based on the students' feedback and discussions. We also discussed the experiment in a half-day meeting with our team of eight

information security managers. These practitioners commented on the wording and structure of the questions, the motivational text in the cover letter, and the overall meanings of each term. We edited the instrument following the managers' comments and suggestions, and emailed the revised questions to these individuals for a second round of comments. The revised instrument was also presented to an information security research center's executive board (see footnote 5), which comprised five information security managers whose companies funded the research center. After incorporating the changes, we piloted the scenarios and the survey with graduate students in our classes during April–June 2012, using approximately 30 students each time.

INSERT TABLE 2,3, and 4 ABOUT HERE

Empirical Execution

For the final data collection, a mail-in technique was adopted to contact executives and obtain their responses. Using the available contact information for C-level executives at the top 690 companies in Finland, each executive was sent a personally addressed cover letter and a copy of the instrument in Finnish in summer 2012. After the invitation to participate and the survey were sent out, 132 completed responses were received over two months, for a response rate of 19.1%. Considering that the addressees were executives at the largest firms in the country, this relatively high response rate was encouraging. Of the total number of respondents, 69 were presidents, chairpersons, or chief executive officers (CEOs; Table 2), and 15 respondents did not report their positions. Of the remaining 117 respondents, there was no IS or security officer, indicating that the majority of respondents fit the profile of a senior executive. More than 100 respondents came from companies with revenues of €50 million (Table 3). All industries in Finland, with the exception of educational services, were represented in the sample (Table 4). Only four companies listed themselves as belonging to the information and communications industry, reasonably ensuring that there was no bias due to tech-savvy executives.

Data Analysis

Each respondent completed five scenarios, resulting in responses for 660 scenarios. Five scenario responses had to be excluded because it was unclear which response was ultimately chosen by the respondent. The remaining responses covered 140 out of the 162 possible scenarios. The number of scenarios completed for each level of *Cost* showed that the responses were uniformly distributed over the various levels, except for the 0.25 cost level (Table 5). Similarly, all values of *Risk*, *Potential Loss*, and *Framing* were included in at least one scenario, indicating fairly random coverage over these variables (Table 6–8).

Tables 5–8 show the mean and standard deviation values for *Support* and *PosDecision* for different values of the independent variables. The mean values for *Support* and *PosDecision* indicate a decreasing trend as the *Cost* increases (Table 5)[6]; this had been expected. It also appears that the mean values of the two indicators differed by level; thus, the different levels elicited different responses from respondents. Tables 6 and 7 show the mean values of *Support* and *PosDecision* for the various levels of *Risk of a Breach* and *Potential Loss from a Breach*. In both cases, the mean values for *Support* and *PosDecision* increased, as expected.

INSERT TABLE 5, 6, 7, and 8 ABOUT HERE

Finally, the mean and standard deviation values of *Support* and *PosDecision* for the two levels of *Framing* are in Table 8. A *t*-test for the difference between the means for *Support* resulted in a value of 0.23 for the *t* statistic, which is less than 1.68 for a one-tailed test, indicating that the difference between the means for *Support* for positive and negative *Framing* were not statistically significantly different from zero. Similarly, a *t*-test showed that the difference between the means of *PosDecision* for the two levels of *Framing* was not statistically significantly different from zero. These two results indicate that the main effect of *Framing* on *Support* and *PosDecision* is not statistically significant.

Measurement Model Test for Latent Variables

The study consisted of three latent variables, *Commitment* at the scenario level and *Rational PSIA* and *Inspirational PSIA* at the respondent level. Thus, a hierarchical linear model (HLM) was used to test the hypotheses. Statistical validity was ensured by checking whether any of the seven indicators for *PSIA* loaded on more than one factor. This was accomplished using a factor analysis of the seven indicator variables with oblique Promax rotation on 132 respondent-level observations, after the minimum eigenvalue criterion was set to one (Table 9).

INSERT TABLE 9 ABOUT HERE

The factor analysis revealed three factors with eigenvalues greater than one, in which *Explain*, *Fact*, and *ROI* loaded on one factor, *Inspire* and *Excite* on another, and *Legit*1 on the third factor (Table 9). *Legit*2 also loaded negatively on *Factor*1, and because a single-item latent variable is not valid in perceptual measures, *Legit*1 and *Legit*2 were dropped (Gefen et al. 2011). Second, a measurement model following traditional structural equations modeling was used to conduct a chi-square test between two models: one where the correlation between *Rational PSIA* and *Inspirational PSIA* was not constrained and one in which the correlation between them was constrained to one (Anderson & Gerbing 1988). The statistically significantly higher model fit of the former model (χ^2 value 205.28; degrees of freedom 7) indicated that the two latent variables were distinct and did not overlap.

The latent variable *Commitment* and its indicators were scenario-level data. Thus, the 655 scenario-level observations were used to determine the number of factors on which *Support* and *PosDecision* loaded. Both indicators loaded on only one factor, with loadings of 0.958 and 0.957, respectively, indicating the high validity of the measurement model. Because *Risk* and *Loss* were ordered categorical variables with three levels each, their categories were coded numerically as 1, 2, and 3, mimicking continuous or interval variables.

Hierarchical Linear Model (HLM)

In the data collected, the scenarios were nested within respondents where *Commitment*, *Risk*, *Loss*, and *Cost* were the scenario-level variables, and *Rational PSIA* and *Inspirational PSIA* were respondent-level variables. Because the research design followed a repeated-measures design in which one respondent evaluated multiple scenarios, the use of the HLM to account for respondent-level effects is warranted. The respondent-level effects included the PSIA constructs, which were calculated as the factor loading-weighted averages of the survey responses, and used the resulting scores for the two variables in the HLM (Bommer et al. 2007). The HLM was run with respondent- and scenario-level variables, and the appropriate interactions between them, specifying the levels of the variables in *xtmixed* in Stata.

The high value for the intraclass coefficient (ρ), 0.599, indicated that a large portion of the variance of *Commitment* was explained by respondent-level variables, and therefore, it is important to include them in the model (Bommer et al. 2007). The Akaike information criterion and the Bayesian information criterion reflected the goodness of the model fit for the HLM. These numbers were smaller for this model compared to a model without the control variables and their interactions, indicating a good model fit.

Because the hypotheses were about the interaction effect of framing, the focus was on the estimates of the interaction effects, and the remaining variables were considered to be control variables (Table 10). The interaction between *Rational PSIA* and *Framing* did not statistically significantly affect *Commitment*. This result meant that the null hypothesis H1 was not rejected, underscoring that a negative tone neither supported the proposal nor backfired with rational executives. The interaction of *Inspirational PSIA* and *Framing* leading to *Commitment* was statistically significantly positive (0.171; $p < 0.001$); thus, H2 was supported.

INSERT TABLE 10 ABOUT HERE

Of the next set of hypotheses for the interactions between the three scenario-level variables and negative framing, the interaction between *Cost of a Solution* and *Framing* affected *Commitment* in a negative fashion; thus, H3 was supported. A negative frame for a proposal amplified the negative impact of the cost of a solution on a senior manager's commitment. The steeper slope of the line for the negative frame estimating the linear relationship between *Commitment* and *Cost* in Figure 2 illustrates this effect. The interactions between *Potential Loss* with *Framing* and *Risk of a Breach* with *Framing* did not affect *Commitment*; thus, H4 and H5 were not supported.

Among the direct effects of the respondent- and scenario-level variables, neither *Rational PSIA* nor *Inspirational PSIA* affected commitment directly. Among the scenario-level variables, *Framing* did not have a direct effect, but the remaining three variables (*Cost of a Solution*, *Potential Loss*, and *Risk of a Breach*) affected *Commitment*. The link between *Cost of a Solution* and *Commitment* was negative, as expected, as commitment decreased with increasing cost. We found positive statistically significant values for the estimates for *Risk* and *Loss*.

Discussion

The empirical analysis showed that the null hypothesis H1 (the lack of impact of the interaction between framing and a rational PSIA on the commitment to information security) was not rejected, and that there was evidence to support hypothesis H2 (the presence of a positive impact of the interaction between negative framing and an

inspirational PSIA on the commitment to information security). There was also support for hypothesis H3, the presence of a negative impact of the interaction between negative framing and cost on the commitment to information security.

As hypothesized, the commitment to information security depends on the interaction between an executive's rational or inspirational PSIA and framing. Negative framing interacts with an executive's inspirational PSIA to drive the executive's commitment to the proposal. Negative framing also interacts with the cost of a security solution such that the commitment to security decreased faster with increases in the cost of the solution in a negatively framed proposal. We had reasoned that the negative framing of a proposal would evoke a higher degree of systematic processing, leading to the evaluation of costs in a more critical manner. The results support this logic.

The lack of a direct effect of PSIA on the commitment to information security for both rational and inspirational PSIA indicates that managers are not predisposed one way or other about spending on information security. For example, a manager of either PSIA is not negatively inclined to information security due to its lack of generating revenues. A similar lack of a direct effect of framing on the commitment to information security indicates that the topic of spending on information security itself does not trigger an aversion or an affinity for a proposal. The lack of direct effects and the presence of interaction effects underscores the confluence of cognitive processing.

The combined results for H2 and H3 indicated countervailing forces that negative framing applies to the commitment of an executive with an average inspirational PSIA to information security. The positive effect from the interaction of negative framing with an inspirational PSIA countered the negative effect from the interaction with the cost of the security proposal. To compare the magnitudes of these effects, consider that the coefficient of cost measures the change in commitment for a 100% (unit) change in cost, and should be appropriately scaled down for changes of less than 100%. Thus, for example, a 10% increase in the cost for negative framing is likely to reduce the commitment to security by –0.2667 (10% of the sum of the coefficients of the cost–framing interaction and the inspirational PSIA–framing interaction, which is –1.958 – 0.709 = –2.667), which is higher in magnitude than the increase in commitment that is possible by the interaction between negative framing and an inspirational PSIA, 0.171 (see Table 10). This result should serve as a caution to managers to not use a negative frame for information security proposals to executives with an average or above average inspirational PSIA, because of the high sensitivity of such executives to the cost of a solution.

The commitment to information security did not change for the interactions of risk and loss with negative framing. This lack of change in commitment may be attributed to the intangible nature of risk and potential loss compared to the tangibility of the cost of a solution, as well as its immediacy. Risk and potential loss, by their very nature, are estimates, and executives may make allowances for variations in these quantities. However, the cost may be perceived to be deterministic. Negative framing of proposals through its interaction effects decreases the chances of the acceptance of an information security proposal for executives with a high inspirational PSIA. If negative framing is used by security managers to talk about information security to executives with a high inspirational PSIA, this could explain some of the problem of inadequate investment that we observe in information security.

Implications for Theory

The model developed in this study used the HSM as the overarching logic for the hypotheses on allocating resources for information security. The newly developed construct PSIA and the framing of security proposals were shown to underlie a mechanism that predicts the commitment to information security proposals. By associating an executive's PSIA with cognitive processing, this study advanced a context-specific route for cognitive processing, which depends on the message and the receiver of the message. The conceptual takeaway for allocating resources for information security is that negative framing may have a more dramatic effect for emotional executives and a less dramatic effect for rational executives. The lack of direct effects of framing and the PSIA on commitment underscores the moderating effect of these two constructs. Finally, the differences between the interaction of cost with framing versus risk and potential loss with framing clearly brings out the nuanced differences among risk, cost, and potential loss in the security context. In summary, the logic captured by the model contributes to the literature on executives' allocation of resources for information security by suggesting a cognitive processing–based approach.

Limitations and Future Research

As with all field studies, a limitation of this study is that the final sample was biased toward large companies. This is not necessarily a drawback because the executives in these companies were further removed from daily IT-

related decisions than their peers in smaller companies, and thus, were likely to show greater variance in information security responses. Nevertheless, future research should examine the possible differences between small and large organizations. A second limitation is that only two types of PSIAs and framing were examined. There are likely other PSIA types and cognitive biases that are relevant in this context. The use of a manager as the unit of analysis is a limitation in the allocation of resources for information security. A model was developed for a manager rather than an organization because the trade press recommended that the chief information security officer (CISO) should have one-on-one engagements with executives first (Ponemon Institute 2014). However, although CISOs often do not communicate with executives, it may be necessary to examine the interaction dynamics between the CISO and executives using case studies. Similarly, the group dynamics of executives should also be examined in an interview-based setting. Next, the presentation of the information security proposal in a concise and quantitative manner may not reflect real-world examples. Although the concise scenarios characterized the essential elements of security investments, it may be not possible to extend the results to cases in which the proposal is descriptive and qualitative. Future research should address these limitations by examining written investment proposals, documenting executive decision making, and interviewing executives who have made investment decisions about IS security. These methods naturally have their own limitations.

Implications for Practice

The results underscore the need to broaden the current analyses of behavioral approaches to information security and prescriptions for managers to cover cognitive biases and PSIA. Practitioners' reports prescribe tactics to information security managers for communicating funding needs to executives. Prescriptions include "know the executive audience," attempt one-on-one interactions using short communications, combine an analytical approach with an emotional approach, and put a positive spin on security issues (Brandel 2012, Duffy 2002, Masters 2012). The findings add to what has been prescribed. First, one aspect of "know the executive" is understanding what his or her leadership PSIA is, because the executive's PSIA is a key moderator in his or her disposition to information security proposals. Second, short one-on-one communications in which risk, cost, and potential losses are expressed quantitatively are useful to preempt apathy toward security issues. Finally, the use of positive and negative frames can also affect the influence of the cost of a security solution on an executive's commitment to information security. With a negatively framed proposal, the increasing cost of a security solution jeopardizes the proposal more rapidly. If the cost of the information security solution is high, then a positively framed proposal may fare better.

Conclusion

Resource allocation in information security is a high-priority problem for researchers and practitioners of information security management (Ernst & Young 2012). This problem has been addressed by researchers normatively as a problem of determining the optimal amount of investment in information security (Gordon & Loeb 2002). As is the case with normative models, simplifying assumptions were made. To address the limitations of simplifying assumptions, the concept of an executive's PSIA was developed, and a behavioral economics and cognitive psychology perspective was adopted to examine cognitive biases in executives' commitment to information security proposals. An empirical validation was conducted by testing negatively and positively framed security investment scenarios with executives, while also observing their rational PSIA and inspirational PSIA. The results showed that at least in the settings of the field experiment, when one has a difficult message such as a high cost, the more effective approach might be to avoid approaches that trigger systematic processing. Thus, decision-maker biases and differences in the PSIA must be taken into account to further understand predisposition to invest in information security.

REFERENCES

Anderson, C.L., Agarwal, R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34, 3 (2010), 613-643.

Anderson, J. C., Gerbing, D. W. (1988). Structural equation modeling in practice: A review & recommended two-step approach. *Psychological bulletin*, *103*(3), 411.

Anderson, R., Moore, T. The economics of information security. *Science*, 314, 5799 (2006), 610-613.

Armacost, R.L., Hosseini, J.C., Morris, S.A., Rehbein, K.A. An Empirical Comparison of Direct Questioning, Scenario, & Randomized Response Methods for Obtaining Sensitive Business Information. *Decision Sciences*, 22, 5 (1991), 1073-1090.

Baskerville, R. Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, 1, 2 (1991), 121-130.

Block, L.G., Keller, P.A. When to accentuate the negative: The effects of perceived efficacy & message framing on intentions to perform a health-related behavior. *Journal of Marketing Research* (1995), 192-203.

Bloomberg Bussinessweek 2014. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data, last accessed January 1st, 2015.

Bommer, W.H., Dierdorff, E.C., Rubin, R.S. 2007. Does prevalence mitigate relevance? The moderating effect of group-level OCB on employee performance, *Academy of Management Journal* (50:6), pp. 1481-1494.

Brandel, M. What I learned when I left security, http://www.csoonline.com/article/707589/what-i-learned-when-i-left-security, June 04, 2012, last accessed October 13th, 2012. (2012).

Cacioppo, J.T., Petty, R.E. The need for cognition. *Journal of personality & social psychology*, 42, 1 (1982), 116.

Cacioppo, J.T., Petty, R.E., Kao, C.F., Rodriguez, R. Central & peripheral routes to persuasion: An individual difference perspective. *Journal of personality & social psychology*, 51, 5 (1986), 1032.

Chaiken, S. Heuristic versus systematic information processing & the use of source versus message cues in persuasion. *Journal of personality & social psychology*, 39, 5 (1980), 752.

Chaiken, S., Maheswaran, D. Heuristic processing can bias systematic processing: effects of source credibility, argument ambiguity, & task importance on attitude judgment. *Journal of personality & social psychology*, 66, 3 (1994), 460.

Chenhall, R., Morris, D. (1991). The effect of cognitive style & sponsorship bias on the treatment of opportunity costs in resource allocation decisions. *Accounting, Organizations & Society*, *16*(1), 27-46.

Cox, D., Cox, A.D. Communicating the consequences of early detection: The role of evidence & framing. *Journal of Marketing*, 65, 3 (2001), 91-103.

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

Deutsch, R., Strack, F. Duality models in social psychology: From dual processes to interacting systems. *Psychological Inquiry*, 17, 3 (2006), 166-172.

Duffy, D. Let's Talk: Security Leadership & Executive Communication, The CSO's guide to strategic executive communication, http://www.csoonline.com/article/217294/let-s-talk-security- leadership-and-executive-communication, September 04, 2002, last accessed October 13th, 2012. (2002).

Dutta, A., McCrohan, K. Management's Role in Information Security in a Cyber Economy, *California Management Review*, 45, 1(2002), 67-87.

E&Y. http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf. (2013).

Epstein, S. Cognitive-experiential self-theory. *Advanced personality*: Springer, 1998, pp. 211-238.

Evans, J.S.B. In two minds: dual-process accounts of reasoning. *Trends in cognitive sciences*, 7, 10 (2003), 454-459.

Evans, J.S.B. Dual-process theories of reasoning: Contemporary issues & developmental applications. *Developmental Review*, 31, 2 (2011), 86-102.

Fagley, N., Miller, P.M. The Effect of Framing on Choice Interactions with Risk-Taking Propensity, Cognitive Style, & Sex. *Personality & Social Psychology Bulletin*, 16, 3 (1990), 496-510.

Fagley, N.S., Miller, P.M. Framing effects & arenas of choice: Your money or your life? *Organizational Behavior & Human Decision Processes*, 71, 3 (1997), 355-373.

Gefen, D., Straub, D.W., Rigdon, E.E. An update & extension to SEM guidelines for admnistrative & social science research. *MIS Quarterly*, 35, 2 (2011), iii-xiv.

Gordon, L.A., Loeb, M.P. The economics of information security investment. *ACM Transactions on Information & System Security (TISSEC)*, 5, 4 (2002), 438-457.

Grewal, D., Gotlieb, J., Marmorstein, H. The moderating effects of message framing & source credibility on the price-perceived risk relationship. *Journal of Consumer Research* (1994), 145-153.

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

Henderson, J. C., Nutt, P. C. (1980). The influence of decision style on decision making behavior. *Management Science*, *26*(4), 371-386.

Hodgkinson, G.P., & Healey, M.P. Psychological foundations of dynamic capabilities: reflexion & reflection in strategic management. *Strategic Management Journal*, 32, 13 (2011), 1500-1516.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management & organizational culture. *Decision Sciences*, *43*(4), 615-660.

Huang, C.D., Hu, Q., & Behara, R.S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, 114, 2 (2008), 793-804.

Jasso, G. Factorial survey methods for studying beliefs & judgments. *Sociological Methods & Research*, 34, 3 (2006), 334-423.

Johnston, A.C., & Warkentin, M. Fear Appeals & Information Security Behaviors: An Empirical Study. MIS *Quarterly*, 34, 3 (2010).

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

Kahneman, D. *Thinking, fast & slow*. Macmillan, 2011.

Kanouse, D.E., & Hanson Jr, L.R. Negativity in Evaluations, in. *Attribution: Perceiving the Causes of Behavior*: Jones E. E. et al. (Eds.), Morristown, NJ: General Learning Press, 1972.

Kipnis, D., Schmidt, S.M., & Wilkinson, I. Intraorganizational influence tactics: Explorations in getting one's way. *Journal of Applied psychology*, 65, 4 (1980), 440.

Kipnis, D., & Schmidt, S.M. Upward-influence styles: Relationship with performance evaluations, salary, & stress. *Administrative Science Quarterly* (1988), 528-542.

Levin, I.P., Gaeth, G.J., Schreiber, J., & Lauriola, M. A new look at framing effects: Distribution of effect sizes, individual differences, & independence of types of effects. *Organizational Behavior & Human Decision Processes*, 88, 1 (2002), 411-429.

Magnusson, C, Molvidsson, J. & Zetterqvist, S., 2007, in *IFIP International Federation for Information Processing*, Volume 232, New Approaches for Security, Privacy & Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J.. von Solms, R.. (Boston: Springer), pp. 25–35.

Mahoney, K.T., Buboltz, W., Levin, I.P., Doverspike, D., & Svyantek, D.J. Individual differences in a within-subjects risky-choice framing study. *Personality & Individual Differences*, 51, 3 (2011), 248-257.

March, J.G., & Shapira, Z. Managerial perspectives on risk & risk taking. *Management Science*, 33, 11(1987), 1404-1418.

Masters, G. RSA Conference 2012: Breaches help in C-suite communication, February 29, 2012, http://www.scmagazine.com/rsa-conference-2012-breaches-help-in-c-suite- communication/article/229998/ last accessed October 14th, 2012. (2012).

Meyers-Levy J, Maheswaran D. Exploring message framing outcomes when systematic, heuristic, or both types of processing occur. *Journal of Consumer Psychology*. 2004 Apr;14(1 & 2):159-67.

Michael, J. (2003). Using the Myers-Briggs type indicator as a tool for leadership development? Apply with caution. *Journal of Leadership & Organizational Studies*, *10*(1), 68-81.

Miller, P.M., & Fagley, N.S. The effects of framing, problem variations, & providing rationale on choice. *Personality & Social Psychology Bulletin*, 17, 5 (1991), 517-522.

Ponemon Institute. 2014. Cyber Security Incident Response: Are we as prepared as we think? Ponemon Institute research Report. http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf, last accessed on November 5th, 2014.

Puhakainen, P. *Design Theory for Information Security Awareness*, 2006. Ph.D Thesis, the University of Oulu, Finland.

Rothman, A.J., Salovey, P., Antone, C., Keough, K., & Martin, C.D. The influence of message framing on intentions to perform health behaviors. *Journal of Experimental Social Psychology*, 29, 5 (1993), 408-433.

Rothman, A.J., & Salovey, P. Shaping perceptions to motivate healthy behavior: the role of message framing. *Psychological bulletin*, 121, 1 (1997), 3.

Shiloh, S., Salton, E., & Sharabi, D. Individual differences in rational & intuitive thinking styles as predictors of heuristic responses & framing effects. *Personality & Individual Differences*, 32, 3 (2002), 415-429.

Simon, A.F., Fagley, N.S., & Halleran, J.G. Decision framing: Moderating effects of individual differences & cognitive processing. *Journal of Behavioral Decision Making*, 17, 2 (2004), 77-93.

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

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

Sloman, S.A. The empirical case for two systems of reasoning. *Psychological bulletin*, 119, 1 (1996), 3.

Smith, E.R., & DeCoster, J. Dual-process models in social & cognitive psychology: Conceptual integration & links to underlying memory systems. *Personality & social psychology review*, 4, 2 (2000), 108-131.

Smith, S.M., & Levin, I.P. Need for cognition & choice framing effects. *Journal of Behavioral Decision Making*, 9, 4 (1996), 283-290.

Stanovich, K.E., & West, R.F. Individual differences in reasoning: Implications for the rationality debate? *Behavioral & brain sciences*, 23, 5 (2000), 645-665.

Stanton, J.M., Stam, K.R., Mastrangelo, P., & Jolton, J. Analysis of end user security behaviors. *Computers & Security*, 24, 2 (2005), 124-133.

Statman, M., Thorley, S., & Vorkink, K.. Investor overconfidence & trading volume. *Review of Financial Studies*, 19, 4 (2006), 1531-1565.

Taylor, S. E. Asymmetrical Effects of Positive & Negative Events: The Mobilization-Minimization Hypothesis. *Psychological Bulletin* (1991),110, I, 67-85.

Thaler, R.H. Anomalies: Saving, fungibility, & mental accounts. *The Journal of Economic Perspectives* (1990), 193-205.

Toplak, M. E., West, R. F., & Stanovich, K. E. (2011). The Cognitive Reflection Test as a predictor of performance on heuristics-and-biases tasks. *Memory & cognition*, *39*(7), 1275.

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

Tversky, A., & Kahneman, D. Loss aversion in riskless choice: A reference-dependent model. *The Quarterly Journal of Economics*, 106, 4 (1991), 1039-1061.

Volkema, R. J., & R. H. Gorman (1998). The influence of cognitive-based group composition on decision-making process & outcome. *Journal of Management Studies*, *35*(1), 105-121.

Vroom, C., & Von Solms, R. Towards information security behavioural compliance. *Computers & Security*, 23, 3 (2004), 191-198.

Wang, J., Chaudhury, A., & Rao, H.R. Research Note-A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, 19, 1 (2008), 106-120.

Yukl, G., & Falbe, C.M. Influence tactics & objectives in upward, downward, & lateral influence attempts. *Journal of Applied psychology*, 75, 2 (1990), 132.

Yukl, G., & Tracey, J.B. Consequences of influence tactics used with subordinates, peers, & the boss. *Journal of Applied psychology*, 77, 4 (1992), 525.

Yukl, G., Seifert, C.F., & Chavez, C. Validation of the extended influence behavior questionnaire. *The Leadership Quarterly*, 19, 5 (2008), 609-621.

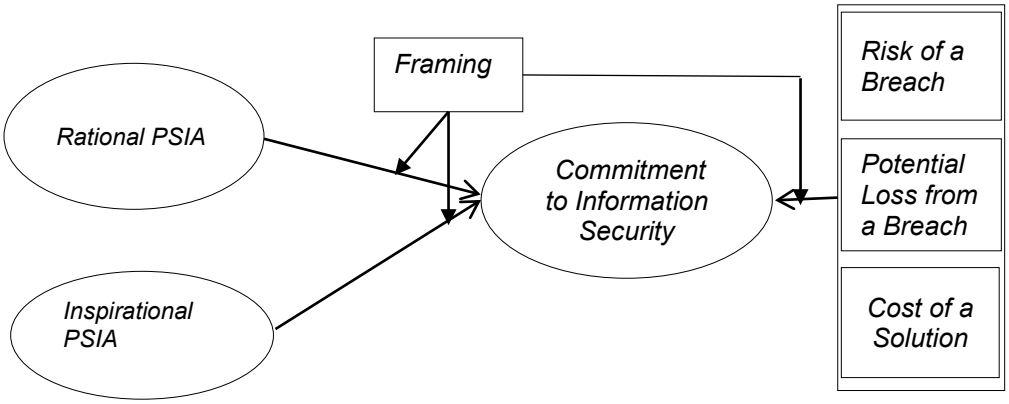

Figure 1. PSIA, Commitment, and Information Security Investment Characteristics

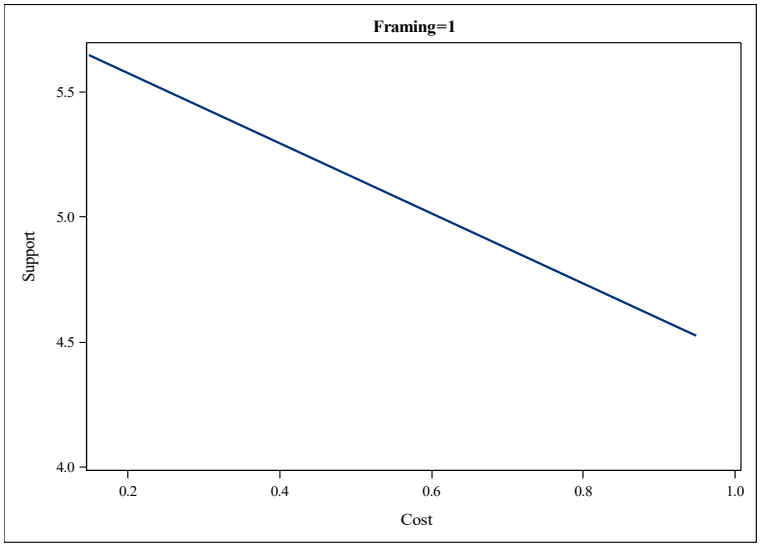

Figure 2. Interaction of Framing on the Commitment and Cost Relationship

Table 1. Three Main Elements of the Scenarios and the Survey Instrument

A. Template for Scenario Depiction in the Scenarios	Variable
• Organizations face a _____<LOW, MEDIUM, HIGH> risk of an information breach targeting highly confidential information.	*Risk*
• This information security breach leads to a _____<LOW, MEDIUM, HIGH> loss of business value for the organization.	*Loss*
• The cost of the information security solution (whether technical or managerial) is ___ <5% to 95% in increments of 10%> of the loss of business value.	*Cost*
• _____<INVESTING, NOT INVESTING> in the solution makes us <LESS VULNERABLE, MORE VULNERABLE> to an information security breach.	*Framing*

Note: The words between < and > in the template above list the possible values for the treatment. For example "<LOW, MEDIUM, HIGH>" in the scenario for *risk* indicates that one of these levels is randomly placed in the actual scenario that a respondent sees.

B. Commitment Statement on the Survey

How likely is it that you will COMMIT to the activity/project? Please circle 1 through 7 for each statement. If you do not know how you would react to the proposed activity/proposal, circle 4.

		Very Unlikely						Very Likely
1.	I would commit to this request.	1	2	3	4	5	6	7
2.	I would make a positive decision about this request.	1	2	3	4	5	6	7

C. Questions about the PSIA (1–7 Likert Scale)	Indicator	Style
1. Use of facts and logic to justify the proposal	*Fact*	*Rational*
2. Evidence of a positive return on investment (ROI) from the proposal	*ROI*	
3. Portrayal of the activity as something exciting and worthwhile	*Excite*	*Inspirational*
4. An inspiring vision of what the proposed activity could accomplish	*Inspire*	
5. Consistency with official rules and policies*	*Legit1*	*Legitimacy**
6. Explanation of how the requested change is necessary to attain the company's business goals*	*Explain*	*Rational*
7. Inconsistency of the proposal with previous precedent and established practice*	*Legit2*	*Legitimacy**

* represents the item or construct eventually dropped after the data analysis because of cross-loading.

Note: Adapted from Yukl et al. (2008), but elicits the preferred way to be presented with a proposal. See supplemental documents for the actual instrument sent to respondents.

Table 2. Ranks of Respondents Represented in the Sample

Rank	Count
President	69
Vice President	13
Member of the Board	11
Director	2
Asst./Dep. Director	18
Chief Information Officer	4
Others/Not reported	15
Total	132

Table 3. Company Size

Revenues (million €)	Count
≥100	78
50–100	45
30–50	6
10–30	3
Total	132

Table 4. Industry Representation in the Sample[7]

Industry/segment	Count	Industry/segment	Count
Agriculture, Forestry, & Fishing	2	Information & Communication	4
Manufactured Products	35	Financial & Insurance Services	1
Electricity, Gas, Steam, & A/C	11	Real Estate	3
Water Supply	2	Professional/Scientific/Tech.	1
Construction/Construction Works	9	Administrative & Support	1
Sewerage, Waste Mgmt. & Remediation	9	Public Admin. & Defense	1
Wholesale & Retail Trade	26	Human Health & Social Work	4
Transportation & Storage	5	Arts, Entertainment, & Recreation	8
Accommodation & Food	1	Other/Unreported	9
		Total	132

Table 5. Distribution of *Cost of a Solution*

Level of *Cost*	N	*Support* Mean	*Support* Std Dev	*PosDecision* Mean	*PosDecision* Std Dev
0.15	73	5.56	1.34	5.38	1.46
0.35	104	5.37	1.39	5.15	1.59
0.45	78	5.14	1.69	4.91	1.67
0.55	76	4.86	1.66	4.81	1.64
0.65	84	4.23	1.84	3.97	1.83
0.75	79	4.65	1.83	4.53	1.93
0.85	74	4.59	1.79	4.36	1.77
0.95	87	4.24	1.98	4.16	1.95

Table 6. Distribution of *Risk of a Breach*

Level of *Risk*	N	*Support* Mean	*Support* Std Dev	*PosDecision* Mean	*PosDecision* Std Dev
LOW	211	4.23	1.81	4.03	1.80
MEDIUM	223	4.92	1.67	4.75	1.70
HIGH	221	5.36	1.58	5.20	1.67

Table 7. Distribution of *Potential Loss from a Breach*

		Support		*PosDecision*	
Level of *Loss*	N	Mean	Std Dev	Mean	Std Dev
LOW	222	4.30	1.81	4.16	1.85
MEDIUM	219	4.90	1.61	4.75	1.66
HIGH	214	5.35	1.67	5.12	1.73

Table 8. Distribution of *Framing*

		Support		*PosDecision*	
Framing	N	Mean	Std Dev	Mean	Std Dev
POSITIVE	333	4.86	1.75	4.67	1.81
NEGATIVE	322	4.83	1.74	4.67	1.77

Table 9. Rotated Factor Pattern of Respondent Data (Standardized Regression Coefficients)

	*Factor*1	*Factor*2	*Factor*3
Fact	–0.126	**0.530**	0.061
ROI	0.053	**0.619**	–0.275
Explain	0.136	**0.788**	0.242
Excite	**0.763**	–0.168	0.268
Inspire	**0.853**	–0.026	–0.087
Legit1	0.019	0.117	**0.919**
*Legit*2	–0.517	–0.304	0.179

Table 10. Estimates of Hierarchical Linear Model Analysis of Figure 1

Variable	Est.	Err.
Intercept	3.774	0.21***
Rational PSIA × *Framing*♣	0.002	0.08
Inspirational PSIA × *Framing*	0.171	0.08**
Cost of a Solution × *Framing*	–0.709	0.36*
Risk of a Breach × *Framing*	0.041	0.13
Potential Loss × *Framing*	–0.018	0.12
Control Variables		
Rational PSIA	–0.001	0.11
Inspirational PSIA	0.026	0.11
Framing♣	–0.060	0.08
Cost of a Solution	–1.958	0.17***
Risk of a Breach	0.552	0.05***
Potential Loss from a Breach	0.534	0.05***
Variance of the respondent-level residual (τ_{00})	1.469	0.20***
Variance of the scenario-level residual (τ_{11})	0.982	0.06***
Intra-class coefficient (ρ)	0.599	
Akaike information criterion (AIC)	2152.1	
Bayesian information criterion (BIC)	2192.5	

*p<0.05; **p<0.01; ***p<0.001;
♣: *Framing* is coded as 1 for negative, 0 otherwise.

About the Authors

Nirup M. Menon obtained his PhD in MIS from University of Arizona, and has taught at Texas Tech University, University of Texas at Dallas, and Instituto de Empresa Madrid prior to joining George Mason University. He is currently a Professor. He has published in *MIS Quarterly*, *Management Science*, and *Information Systems Research*, among other journals, and is an AIS, IEEE, and INFORMS member.

Mikko T. Siponen is a professor and Vice Dean for Research at the University of Jyvaskyla, Finland. He has four different postgraduate university degrees, of which two are doctoral degrees. His research interests include IS security, philosophical aspects of IS, and software development. He has published more than 60 articles in journals such as *MIS Quarterly* and *Information Systems Research*. He has received over 10 million EUR of research funding from corporations and numerous funding bodies.

[1] Based on www.privacyrights.org, accessed July 14, 2018.

[2] Borrowing from this literature, we also included legitimating as a PSIA during data collection; however, we excluded its indicators because of cross-loading. Although the other influence styles not considered here may play a role in organizations' security investment, they are context-specific (e.g., the exchange influence, in this context, would mean that a security manager engages in a *quid pro quo* arrangement with an executive), and it is not clear that an executive would prefer that a subordinate use such an influence style.

[3] We consider this research design to be an experiment, because we manipulated several independent variables and randomly assigned participants to the different conditions. Surveys are typically correlational designs in which all variables, exogenous and endogenous, are measured rather than manipulated. In the data collection, only the constructs, the rational PSIA and the inspirational PSIA, were measured and were not manipulated. All other independent variables (framing, risk, loss, and cost) were manipulated.

[4] The research was part of the activities of an information security research center in Finland that is funded by 20 companies. The eight practitioners were considered leading experts by the executive board of the research center. All the experts are well-known in information security circles in Finland.

[5] The remaining two corresponded to legitimacy, one of the influence types from the Yukl et al. 2008 study, but was dropped due to poor measurement statistics.

[6] There was a precipitous drop at the 0.65 cost level in Table 5 that did not fit the otherwise gradual decline in *Support* and *PosDecision* for security over cost. We conjecture that the linear relationship between cost and commitment may be violated here, and deserves further research. We thank an anonymous referee for pointing this out.

[7] Based on industry classifications in Finland (see http://www.stat.fi/index_en.html, last accessed August 21, 2012).