Journal of Management Information Systems
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/mmis20

The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective

Qing Hu, Robert West & Laura Smarandescu
Published online: 15 Apr 2015.

To cite this article: Qing Hu, Robert West & Laura Smarandescu (2015) The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective, Journal of Management Information Systems, 31:4, 6-48, DOI: 10.1080/07421222.2014.1001255

To link to this article: http://dx.doi.org/10.1080/07421222.2014.1001255

The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective

QING HU, ROBERT WEST, AND LAURA SMARANDESCU

QING HU is the Union Pacific Professor in Information Systems and associate dean for graduate programs and research in the College of Business at Iowa State University. He received his Ph.D. from the University of Miami. His research primarily focuses on the impact of information technology on organizational strategy, culture, security, and performance. His work has been published in leading academic journals, including *Information Systems Research, Journal of Management Information Systems, MIS Quarterly, Journal of the AIS, Communications of the ACM, California Management Review, Decision Sciences, IEEE Transactions on Software Engineering, European Journal of Information Systems,* and *Information Systems Journal*. He has served as special issue associate editor for *MIS Quarterly* and *European Journal of Information Systems* and on the editorial board of *Journal of the AIS.*

ROBERT WEST is a professor of psychology at Iowa State University. He completed a doctoral degree in experimental psychology at the University of South Carolina and postdoctoral training in cognitive neuroscience at the Rotman Research Institute in Toronto. He is a fellow of the Association for Psychological Science and the Psychonomic Society. His research uses event-related brain potential and behavioral techniques to examine the neural basis of selective attention, cognitive control, and feedback processing in healthy younger and older adults. His work has been published in leading academic journals, including *Psychological Bulletin, Journal of Cognitive Neuroscience, Neuropsychologia*, and *Cerebral Cortex*. He has served as associate editor of the *Journal of Gerontology: Psychological Sciences* and on the editorial board of several other journals, including *Neuropsychology* and *Psychology and Aging*.

LAURA SMARANDESCU is an assistant professor of marketing in the College of Business at Iowa State University. She is also on the faculty in the Human Computer Interaction Graduate Program. She received her Ph.D. from the

An earlier version of the study was presented at the Forty-Seventh Hawaii International Conference on Systems Science and included in its proceedings. The authors would like to thank Zachary Yaple for assisting with the experiments and collecting the EEG data used in this study, as well as for his comments on the earlier draft of this manuscript that have helped improve the quality of the manuscript. We are also in debted to the three anonymous reviewers and the editorial team for their constructive and insightful comments and suggestions, which have contributed to the quality of this manuscript. This study is partially funded by a bootstrap grant from the College of Business at Iowa State University.

Journal of Management Information Systems / Spring 2015, Vol. 31, No. 4, pp. 6–48.

ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: 10.1080/07421222.2014.1001255

University of South Carolina. She is a member of the interdisciplinary organization Society for Judgment and Decision Making. Her research area is judgment and decision making, and focuses on the effect of environment and individual personality characteristics on decision making and behavior. Her work has been published in leading academic journals in marketing and prevention science, including *Psychology and Marketing, Journal of Advertising Research, Marketing Letters, Marketing Science Institute, Substance Use and Misuse*, and *International Journal of Drug Policy.*

ABSTRACT: Self-control has been identified as a major factor influencing individual behavior in the social science, neuroscience, criminology, and information security literatures. In this study, we first developed and validated a novel paradigm suitable for use with event-related potentials (ERPs) in scenario-based laboratory experiments of decision making in the context of information security. We then used this paradigm to examine the association between individual differences in self-control and ERPs elicited while individuals deliberated over violations of information security policies. Our results show that the left and right hemispheres of the brain were involved in decision making, and that the participants with low self-control had lower levels of neural recruitment in both hemispheres relative to those with high self-control. This was especially the case for regions in or near the dorsal lateral prefrontal cortex (DLPFC) and inferior frontal cortex (IFC). These results extend the findings in neuroscience literature related to the role of self-control in decision making in general, and validate a new paradigm for use with the electroencephalography/event-related potentials (EEG/ERP) technique to examine theoretical questions in information security and criminology research.

KEY WORDS AND PHRASES: information security, neuroscience, self-control, policy compliance, neural correlates, electroencephalography (EEG), event-related potentials (ERPs), NeuroIS.

Human agents have often been identified as the weakest link in the information security defensive chain around the digital assets of an organization [8, 28, 32]. This is because the effectiveness of other elements in security defense, such as security technology, organizational policies and procedures, as well as government regulations and laws, are largely dependent on the effort of human agents, especially those who work with digital assets on a daily basis within organizations. In fact, human agents inside an organization could be as dangerous as, and potentially more dangerous than, those outside the organization due to their intimate knowledge of the organizational information systems and the access they receive either properly or improperly for their routine work activities. In a survey of information technology (IT) managers of global companies, 60 percent of the respondents said that employee misconduct involving information systems is a top concern related to information security, second only to major computer viruses [17].

We define employee security policy violation as any act by an employee using computers that is against the established rules and policies of an organization regardless of the motives. By this definition, security violations include but are not

limited to unauthorized access to data and systems, unauthorized copy or transfer of confidential data, or selling confidential data to a third party for personal gains. Although there is a rich body of literature on employee security behavior in organizational settings [6, 8, 11, 28, 32, 52, 53], the proposed models and theories differ significantly in terms of perspectives and prescriptions. Whereas each of the prior studies focuses on different theoretical aspects of the similar underlying phenomenon, we recognize that there is at least one significant gap in the behavioral research on information security: the role of relatively stable individual characteristics has not been adequately addressed in published studies. For example, some widely recognized individual characteristics, such as self-control and moral beliefs that are frequently associated with criminal or deviant behavior in the criminology literature [1, 9, 50], have attracted limited attention in the information systems literature (e.g., 27, 29).

Can we predict which employees would be more rule-abiding when entrusted with sensitive and valuable digital assets in organizations based on their individual characteristics? Do we know why some employees are better than others at resisting the temptation of short-term gain in order to achieve more significant long-term benefits? There is a plethora of theories in management, economics, and psychology regarding human motivation and behavior in the context of information security (e.g., 8, 11, 27, 32, 52, 59). However, most of these studies are based on interviews and surveys that rely on self-reporting, which has been plagued with issues like common method bias or social desirability [47]. Recent advances in cognitive neuroscience, however, provided a unique opportunity to study human behavior without many of the biases common in the traditional behavioral research literature [14, 55].

We believe that a neuroscience perspective can make a significant contribution to our understanding of human behavior and decision making in the context of information security. Brain imaging technologies, such as functional magnetic resonance imaging (fMRI) and electroencephalography (EEG), enable researchers to measure neural activity in the human brain while research participants are contemplating various decisions, and thereby to establish the neural correlates of the decision processes. Perhaps more interesting to social scientists, the neurocognitive approach and utilization of brain imaging technologies may significantly reduce social desirability biases in participant responses because neural processes are difficult to be consciously manipulated by the participants. By directly measuring the brain processes, brain imaging tools offer more objective or unbiased measurement of decision-making, cognitive, emotional, and social processes [14]. In recent years, the neuroscience perspective has attracted significant attention from information systems (IS) scholars [7, 10, 14, 55], and neuroscientific methods have been applied to a wide range of information systems research issues and shed some interesting light on familiar topics or phenomena, such as trust [5, 13, 49], emotion [21], user beliefs [22], online buying [35], information processing [42], and information security [55].

We conducted two studies using event-related brain potentials (ERPs)—an index of the activity of populations of cortical neurons measured at the scalp to sensory, cognitive, or motor stimuli—to investigate the neural basis of human decision making related to rule- abiding/breaking behavior in the context of information security. We addressed the following research questions in this study:

R1: What is the neurological basis of individual decision making in a scenario-based information security research paradigm?

R2: What are the behavioral differences between low- and high-self-control individuals in the context of information security–related decisions?

R3: What are the neurological differences between low- and high-self-control individuals in the context of information security–related decisions?

Studies using ERPs require experimental paradigms that can reliably elicit neural responses to task-relevant stimuli. Given the novelty of this study, we found no established paradigms in the literature that could serve as a model for it. Therefore, we conducted two ERP studies in order to accomplish our objectives and address the research questions. In Study 1 we examined the ERPs elicited during completion of the new experimental paradigm to validate the efficacy of scenario-based tasks for use with this methodology. In Study 2 we used this new paradigm to examine the neural basis of individual differences in self-control on the neural correlates of decision making related to information security policies.

What we found in this study is interesting and significant to information security research. In addition to validating a novel ERP paradigm for studying individual behavior in the context of information security and potentially criminology, three important results emerged from this research. First, we show that the instrument of Grasmick et al. [20] for measuring self-control in criminology can be used in neuroscience research as a valid measure of self-control. This opens numerous research opportunities for information systems and criminology scholars to use neuroscience theories, methodologies, and tools. Second, we find that self-control as measured by Grasmick et al. [20] is indeed associated with neural activity in the brain, and thus it is not merely a behavioral characteristic but also a neurological characteristic of individuals. This finding questions some conventional wisdom in criminology and information security, and calls for new perspectives on the effectiveness of training in preventing and correcting deviant and criminal behavior. Last but not least, we observed two patterns of neural recruitment related to individual differences in self-control: one reflected differential recruitment by low- and high-self-control individuals, and the other reflected reduced neural recruitment in low-self-control individuals relative to high-self-control individuals. Whereas some of these findings are consistent with the extant literature in neuroscience about neurological mechanisms of self-control, they are the first such findings reported in the criminological and information security literatures. We hope this study will inspire more criminology

and information systems scholars to adopt theories and methodologies grounded in the neuroscience perspective.

Theoretical Background

The concept of self-control in human decision making has fascinated philosophers and scientists alike throughout recorded history because the ability to exercise self-control is essential to the success and well-being of mankind [23]. Self-control is defined in general as the exertion of control by one over the self [44]. In the context of criminology and information security, we follow Gottfredson and Hirschi [19] and define self-control as an individual's ability to refrain from committing deviant or criminal acts under given circumstances. Self-control has attracted significant interest from psychologists [15, 33], criminologists [1, 19, 20, 57], neuroscientists [23, 31, 40], and, more recently, information security scholars [27, 29]. The process of self-control occurs when a person attempts to change the way he or she would otherwise react to stimuli or circumstances [44]. It is generally agreed that self-control is designed to maximize the long-term best interests of the individual, and people exert self-control when they follow rules or inhibit desire for immediate gratification [44]. In the following sections, we briefly review three streams of research on self-control that are relevant to our research questions.

Self-Control and Deviant Behavior

In criminology, one of the preeminent theories is self-control theory [19]. This "general theory of crime" was developed to explain a wide range of criminal activity in society. Gottfredson and Hirschi [19] argued that all human beings have the same potential for committing crimes given the right circumstances; however, not everyone becomes a criminal because of individual differences in self-control. This ability is thought to be established early in life and remains relatively stable throughout the lifespan [19]. Criminal behavior is likely to occur when an individual with low self-control is presented with the opportunity to commit a crime. Gottfredson and Hirschi [19] further argued that individuals with low self-control have a tendency to respond to tangible stimuli in the immediate environment because they usually have a "here" and "now" orientation, and are also more likely to be seduced by the thrill and excitement of committing deviant or criminal acts.

Since its introduction, self-control theory has become a dominant framework in criminology [12], and has accumulated strong empirical support [46]. Low self-control has been found to have direct and indirect influence on criminal behavioral intentions. For example, in a study of shoplifting behavior in college students, Piquero and Tibbetts [46] found that low self-control not only has a direct effect on the intention to shoplift but also indirectly affects the intention through situational variables (e.g., pleasure and shame). Vazsonyi et al. [56] found that low self-control is directly linked to a number of deviant behaviors in both genders and across

different age groups, and that the effects appear to be country and culture invariant in a large-scale study of youth in four countries. Wright et al. [58] also provided strong evidence for the critical role of low self-control in adult criminal behavior and behavioral intention in a study based on longitudinal data of individuals from ages five to twenty-six. Overall, the criminology literature has been fairly consistent and supportive of the significant role of self-control in criminal or deviant behavior at the individual level.

Self-Control and Violations of Information Security

Because criminal acts can be attributed to the individual characteristic of self-control, it follows that "offenders commit a wide variety of criminal acts, with no strong inclination to pursue a specific criminal act or a pattern of criminal acts to the exclusion of others" [19, p. 91]. This provides the foundation for IS scholars to use the theory for understanding information security offenses committed by individuals. Higgins et al. [26] were among the earliest investigators to use self-control in studying individual behavior in the information security context. Using undergraduates and a factorial design, the authors found that low self-control, along with certainty of deterrence, were significantly associated with software piracy. Similarly, Zhang et al. [60] tested the impact of self-control and deterrence on digital piracy (e.g., illegal copying of digital products such as software, documents, video, and audio) in college students. The authors found that only the risk-taking dimension of low self-control and the certainty dimension of the deterrence had a significant impact on the focal behavior. Hu et al. [27] provided more direct evidence by using survey data of employees and contrasting the effect of self-control, moral belief, and deterrence on the employees' intention to violate information security policies in organizational settings. They found that low self-control was the strongest contributor to the intention, primarily through affecting employees' perception of intrinsic and extrinsic benefits of the violations based on a rational choice behavioral model. These studies support the argument that self-control is indeed an important factor in understanding information security policy compliance or noncompliance behavior of employees in organizational settings.

Neural Correlates of Self-Control

The concept of self-control has also attracted the attention of neuroscientists interested in human decision making and social behavior. This is because the human ability to resist temptations for pursuing immediate self-interest has been suggested as a hallmark of civilization [34]. In the neuroscience literature, self-control is more narrowly defined and frequently labeled as "resistance to temptation" [38], "inhibitory control" [2], "impulse control" [40], and other similar terms. In this body of literature, it is generally believed that self-control results from interactions among

different neural circuits. In a study designed to examine interactions between the neural systems underpinning self-control, stimulus valuation, and decision making, Hare et al. [23] argued that goal-directed decisions have their basis in a value signal encoded in the ventromedial prefrontal cortex (vmPFC), and that self-control involves modulation by the dorsolateral prefrontal cortex (DLPFC) of the value signals computed in the vmPFC. These arguments are supported by their study of brain activity using fMRI while dieters engaged in real decisions about food consumption. They found that activity in the vmPFC was correlated with goal values regardless of the amount of self-control exercised by the participants; however, it incorporated both taste and health signals in self-controllers but only taste signals in non–self-controllers. More importantly, activity in the DLPFC increased when the participants exercised self-control and correlated with activity in the vmPFC. Based on these results, Hare et al. [23] speculated that the vmPFC might have originally evolved to forecast the short-term value of stimuli but humans eventually developed the ability to incorporate long-term considerations into values by giving structures such as the DLPFC the ability to modulate the basic value signal. Therefore, a fundamental difference between successful and failed self-control might be the extent to which the DLPFC modulates the vmPFC [23].

Similarly, Lopez et al. [38] found that food-cue reactivity in the ventral striatum, more specifically, the nucleus accumbens (NAcc), a part of the mesolimbic dopamine system associated with reward processing, significantly predicted the strength of food desires, enactment of those desires, and even the amount eaten. But they also found that the inferior frontal gyrus (IFG) is a critical brain region that moderates self-regulatory outcomes, especially when people are faced with strong temptations and self-control is required: those who recruited IFG more during the response-inhibition task tended to be less likely to succumb to temptations and also ate less. The critical role of the IFG in self-control is also confirmed in Aron et al. [2]. Other studies in neuroscience have found more direct relationships between self-control and the prefrontal cortex (PFC), especially the right PFC and the right ventromedial PFC regions [4, 34, 54]. It is fair to say that there is strong neurological evidence to link self-control with neural activity in the vmPFC and DLPFC regions of the human brain.

Studies of self-control using ERPs are relatively rare in the published literature. Inzlicht and Gutsell [30] provided one demonstration of how ERPs may be used to study the effect of variation in self-control or self-regulation. They tested a theory wherein self-control is thought to be implemented by an executive control system in the brain that allows one to detect and resolve conflicts among competing thoughts or response tendencies. Based on this account, failure of self-control occurs when the executive control neural system is depleted due to repeated activation. Support for this idea was found as amplitude of the error-related negativity (ERN) generated in the Stroop task was found to be reduced in a group asked to suppress their emotions while watching two movie clips prior to the test, compared to the control group that was instructed to simply watch the movie clips carefully. While this study establishes a link between self-control and ERP components (i.e., ERN) related to

executive control and decision making, it does not speak directly to the key questions in the domain of information security that represent the focus of the current investigation.

Motivation for Current Research

The extant literature suggests that self-control plays a significant role in human behavior, from economic decisions and social conduct to substance abuse and criminal activity. However, one critical question that is still debated by scholars is how exactly self-control influences human behavior and decision making. Empirical studies based on survey methodology are divided into two camps: those that support a direct effect of self-control on behavior and decision making, and those that support an indirect effect of self-control on behavior and decision making. The direct effect camp argues that individuals with low self-control focus on the excitements and short-term gains and ignore the consequences and long-term costs of deviant actions, and therefore, rational choice and moral judgment models of decision making have little effect because they are bypassed or short-circuited in low self-control individuals when criminal or deviant opportunities are presented [12, 19, 20, 56]. This school of thought is analogous to and consistent with evidence from the neuroscience literature that the PFC region of the brain, especially the right PFC region, underpins self-control [2, 4, 34, 54].

The indirect effect camp, which is more dominant in the criminology literature, argues that rational choice is the fundamental process of human decision making and behavior, and the impact of self-control on human behavior and decision making is through altering the evaluation parameters in rational calculus, such as increasing the perceived benefits and decreasing the perceived costs of intended actions, or interacting with other decision parameters, such as moral values and social learning when criminal or deviant opportunities are presented [27, 46, 50, 51, 57]. This school of thought is analogous to and consistent with neuroscience evidence that self-control is the result of the extent of modulation exerted by the DLPFC on the value signal of the vmPFC for a given stimulus [23] or the moderating effect of IFG on the desire signals generated in NAcc by external stimuli [38].

A significant issue in the extant literature on self-control lies in the measurement of the construct. In the criminology and information systems literature, the scale of Grasmick et al. [20] has been widely adopted, creating a relatively consistent baseline for comparison across studies. This is not the case in studies utilizing neuroscience methodologies where self-control is frequently measured by ad hoc scales. For example, Hare et al. [23] classified high-self-control versus low-self-control participants based on their response to food choices; Martin and Potts [40] used a revised version of the Barratt impulsiveness scale [45]; Lopez et al. [38] used yet another specialized measure of self-control based on the restraint scale [25], and in Inzlicht and Gutwell [30], self-control was not measured but inferred from the amplitude of the ERN. This measurement gap raises an interesting and critical

question for scholars who want to study criminological phenomena in which self-control as measured by Grasmick et al. [20] is a central construct from a neuroscience perspective. If we use the Grasmick et al. [20] measurement for self-control, can we still observe similar neural activity in the brain and its effect on self-control with criminological stimuli? In other words, is the Grasmick et al. [20] measure adequate for studying the effect of self-control in decision making using a neuroscience approach such as brain imaging with EEG or fMRI?

Another critical observation of the literature is that almost all criminology and information security studies involving self-control use survey-based methodology, while almost all studies in neuroscience involving self-control are laboratory-based experiments. Thus, an interesting and critical question is: Can we study self-control in the context of criminology, such as information security policy violations, in a laboratory setting with a controlled experiment using neuroimaging techniques such as EEG or fMRI? In this study, we intend to answer these questions by designing and testing a new paradigm suitable for use with the ERP technique in laboratory-based criminology and information security research, and then testing research hypotheses derived from the three research questions. In doing so, we hope to significantly advance theory and methodology for information security research in specific and criminology research in general.

Research Hypotheses Development

Whereas the two schools of literature disagree on how exactly self-control contributes to deviant behavior, the criminology literature is fairly consistent that low self-control, as measured by Grasmick et al. [20], leads individuals to focus more on short-term reward and less on long-term consequence, thus making them more likely to take risks for immediate gratification [1, 12, 50, 51, 57]. Although self-control is a relatively new concept in information security research, given similarities between deviant behavior in criminology and computer abuse or information security policy violations, it is not a difficult adaptation to use self-control–related theories to explain information security behavior [27, 29].

An ERP study of reward and punishment sensitivity in risky decision making by Martin and Potts [40] showed that the high-risk option was the default choice for high-impulsive participants, while the low-risk option was the default choice for low-impulsive participants. They also found that the low-impulsive participants, but not the high-impulsive participants, had higher ERN following a high-risk choice, indicating that the low-impulsive participants evaluated the risky choice as a poor decision, whereas the high-impulsive participants were less sensitive to the negative consequences of their choices. Hu et al. [27] found that low self-control was the most significant contributor as compared to other factors including moral beliefs and deterrence to employee intention to violate information security policy in organizational settings, primarily through increasing the perceived intrinsic and extrinsic values of the deviant acts. Thus, in situations where violation of established

information security policies may provide immediate reward and only a possibility of punishment in the future, we argue that individuals with low self-control are most likely to focus on the immediate reward and ignore or discount the possibility of more significant future punishment. Therefore, we posit:

> ***Hypothesis 1:*** *Individuals with low self-control tend to choose actions with near-term gain but potential long-term loss in contrast to those with high self-control when contemplating decisions in the context of information security policy violations.*

One of the major characteristics of self-control is impulsivity in individual behavior [20]. Impulsivity by definition means that impulsive individuals, or those with low self-control, do not take adequate time to evaluate input, or in other words, exercise adequate "executive control," before making a decision, as opposed to those with high self-control. There is some degree of consensus among scholars in the area of neuroscience that one of the functions of the PFC region of the brain is broad "executive control" that schedules and optimizes subsidiary processes implemented in the posterior cortical and subcortical regions [43]. In order to exercise "executive control," multiple regions within the PFC and subcortical structures have to be activated [16]. For example, the left lateral PFC underpins the maintenance of goals/sets, the dorsal anterior cingulate cortex (ACC) is responsible for detecting conflicts when the stimuli do not match the goals, and the right inferior frontal cortex (IFC) must suppress irrelevant responses [2]. In order to exert effective self-control or inhibition, the dorsal lateral prefrontal cortex (DLPFC) must be able to modulate the value signals encoded in the ventromedial PFC [23], or the IFG must modulate desire generated by the NAcc [38]. Individuals with low self-control do not sufficiently recruit the DLPFC or IFG [34]. Although we found no direct evidence from studies using neuroscientific or behavioral methodologies for individual differences in decision time related to information security or risk, the findings of the studies above support the argument that it takes time to engage neural mechanisms related to activating, maintaining, and coordinating the processes in order to accomplish self-control. This, coupled with the fact that impulsivity is a major trait of individuals with low self-control, leads to the conjecture that low-self-control individuals may take less time to make a decision than high-self-control individuals due to activation of fewer or weaker neural processes. Thus, we submit that:

> ***Hypothesis 2:*** *Individuals with low self-control tend to make choices faster in contrast to those with high self-control when contemplating decisions in the context of information security policy violations.*

Recent discoveries in neuroscience have generated significant insights into how self-control influences human behavior and decision making. Self-control has been linked to neural recruitment within the DLPFC and the vmPFC [3, 23], especially the right ventromedial prefrontal cortex (rvmPFC) [4, 34, 54], using fMRI. One of

the most interesting findings of these studies is that in patients with lesions of the rvmPFC or right prefrontal region (rPFC), there were significant deficits in social conduct, decision making, risk management, and emotional processing, in comparison to those patients who had only left-side lesions, or to the control groups [9, 54], suggesting a strong link between self-control and the rPFC region of the brain.

Knoch and Fehr [34] provided additional evidence for the role of the rPFC in self-control by using repetitive transcranial magnetic stimulation (rTMS) to temporarily disrupt the brain function in this region during a gambling task measuring risk-taking behavior in healthy adults. They found that individuals with right DLPFC disruption displayed a stronger preference for choosing the larger reward at the risk of even greater penalty, while those with left DLPFC disruptions did not and performed similarly to those with sham treatment. This was corroborated by Boes et al. [4] using healthy school-age boys. They found that neural activity in the rvmPFC was a significant predictor of impulse control ratings provided by parents and teachers of these boys, and fMRI revealed that the rvmPFC volume was significantly lower in the subgroup of impulsive participants compared to the subgroup of non-impulsive ones.

These studies provide strong evidence for us to argue that the behavioral construct self-control is related to the function of the PFC, especially in the rPFC region. Damage to or underdevelopment of the rPFC or rvmPFC is likely to cause an individual to have diminished ability for self-control, as indicated by impulsive behavior, preference for risky choices, or disregard for long-term negative consequences. However, given the fact that this is a study based on EEG technology, which is known to have limited spatial accuracy but high temporal resolution, we shall not make strong location-specific conjectures about self-control and neural activity in the brain, but a more general prediction about the differences in brain activation between low- and high-self-control individuals. This discussion leads to:

> ***Hypothesis 3:*** *Individuals with low self-control tend to exhibit lower levels of neural recruitment in the right hemisphere of the brain than those with high self-control when contemplating decisions in the context of information security policy violations.*

To investigate these hypotheses, we carried out two studies using the ERP technique in combination with a simulated decision-making task grounded in information security policy violations in organizational settings. Although the majority of the reference studies on self-control and behavior in the neuroscience literature use brain-imaging technologies such as fMRI, we chose EEG for two primary reasons. The first and foremost reason is the high temporal resolution of EEG, which is accurate to the millisecond level, in contrast to fMRI, which reflects the slow hemodynamic response that evolves in seconds. The second reason is the low cost of EEG relative to fMRI, which allows researchers to study relatively larger samples in comparison to studies using fMRI [48]. On the other hand, there are some

significant caveats in regard to using EEG technology for brain imaging, which will be discussed later.

Methodology

Participants

Participants for this study were English-speaking undergraduate students attending a large public university in the Midwest, who were recruited from a participant pool of about 350. Students signed up for the research pool voluntarily, and if they were selected for participation in the studies, they received course credit and a small monetary reward. Study 1 aimed at developing and validating the scenario-based ERP paradigm for use in information security research. This study involved 21 (right-handed males, average age 21.86, std. 2.42) student participants randomly selected from the general participant pool. Study 2 aimed to examine the relationship between individual differences in self-control and the ERP correlates of decision making are related to the three research hypotheses. This study involved 40 (right-handed males, average age 21.48, std. 1.97) student participants selected from the general participant pool based on their self-control scores using a survey instrument adapted from Grasmick et al. [20]. The screening instrument is included in Appendix A. Only those participants who had a score in the top 25 percent (low self-control) or bottom 25 percent (high self-control) were invited to participate in Study 2. There was no overlap of participants between the two studies. The reason for using only the participants with the top and bottom self-control scores is to contrast the influence of self-control—the focal variable of this study—on individual decision making. All participants had normal or corrected normal vision, and signed the consent form prior to inclusion in the study.

To motivate truthful responses from the participants, we designed a paradigm that involved some degree of deception, with the approval of our Institutional Review Board. All participants in the general pool were invited to take a 68-item survey that include demographic data, self-control measurement, moral judgment, and decisions related to three information security policy violation scenarios. At the beginning of the experiment, each participant was informed that a computer program had developed a psychological profile based on his responses to the survey, and that he would be paid anywhere from $15 to $25 based on how the responses during the study matched the profile. Participants were also told that the best strategy to earn the most money was to answer the questions as truthfully as possible. In fact, there was no psychological profile, and the computer generated randomly an amount between $23 and $25 to pay each participant at the end. The narrow payout range was designed to minimize the psychological effect on participants of the payment that was received. All participants were debriefed about the protocol after the study was completed.

Stimuli

We faced two challenges in designing the paradigm used in the two studies. First, we needed a paradigm that could simulate decision making related to violations of information security policy within the controlled environment of the laboratory. Second, we needed a paradigm where a decision could be elicited by or locked to a relatively simple discrete stimulus in order to capture the ERPs related to decision making.

We addressed the first challenge by adapting the scenario-based approach widely used in criminology and information security research that elicits vicarious responses from ordinary participants in criminal or deviant situations (e.g., 11, 24, 46, 51, 52). Due to the secrecy involved in criminal or deviant behavior, it is natural that individuals are unwilling or uncomfortable about reporting their own deviant or criminal behavior in studies. Traditional questionnaires that rely on self-reporting of deviant or criminal intention or behavior could have questionable reliability. In criminological research, faced with similar difficulties, scholars have often resorted to the use of scenarios of criminal activities to elicit responses from ordinary survey participants.

To simulate real-world situations as closely as possible, before the test stimuli were presented, the participant was primed with a scenario as follows:

> Josh works for the IT department of a large global manufacturing company that supplies sophisticated electronic control instruments for civilian and military uses. Over the years Josh has developed knowledge and skills that enable him to access almost any computer and database in his company with or without authorization.
>
> The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or nonconfidential data.
>
> Josh has been working on multiple projects recently, some with deadlines in one or two weeks. Josh is under tremendous pressure to meet the deadlines of his boss. Josh is also financially stressed and he is behind in some payments for his bills and credit cards.
>
> In all of the following scenarios, imagine that you are Josh …

Based on research literature, media reports, and personal knowledge about information security breach incidents in organizations, we developed 15 scenarios as stimuli in each of the three categories: control, minor violations, and major violations, for a total of 45 stimuli based on information security scenarios. Table 1 provides a definition for each category with a sample scenario for illustration. All test scenarios and stimuli can be found in Appendix B.

We addressed the second challenge with two treatments included in the experiment design. The first treatment was to motivate the participants to be truthful in their

Table 1. Scenarios and Examples

Conditions	Definition	Sample scenario and stimuli
Control	Scenarios involve routine decisions an individual makes in everyday life that do not involve information security and are usually inconsequential.	*Josh's girlfriend Jenny, who works for a consulting firm, asks Josh if he can take a day off this week to help her on a project she needs to complete that week for her firm.* Prompt: Should Josh take a day off to help Jenny?
Minor violation	Scenarios involve decisions an individual makes that are related to information security situations and may have moderate consequences.	*Josh's girlfriend Jenny, who works for a consulting firm, wants to know whether one of her clients is involved in the new product development with his firm.* Prompt: Should Josh access the secure server and find out for Jenny?
Major violation	Scenarios involve decisions an individual makes that are related to information security situations and could have significant consequences.	*Josh's girlfriend Jenny, who works for a consulting firm, wants to have some information about suppliers. Jenny could earn a substantial amount of commission.* Prompt: Should Josh access the secure server and find the data for Jenny?

responses, which was accomplished by a deception procedure embedded in the experiment as described in the previous section. The second treatment was to use repeated trials by presenting the three types of stimuli (control, minor, and major) with 15 different variations each using a pseudorandom order (the order of the stimuli presentation were randomized but consistent across all participants), which is a common technique in studies involving EEG/ERP. All of the stimuli were programmed into the E-PRIME software (PST, Inc., Pittsburgh, PA).

Procedure

When a participant entered the lab at the assigned time slot, the participant was briefed about the study, and instructed to read and sign the consent form. The participant was then directed to the sound-damped and electrically shielded data collection booth and seated in a comfortable armchair. The participant was placed approximately 15–20 inches from the computer monitor that displays the stimuli and decision choices. The EEG cap was then fitted on the head of the participant by the research assistants. EEG data were recorded using the Sensorium Acquire software package. No breaks were given throughout the experiment which usually lasted about 30–35 minutes.

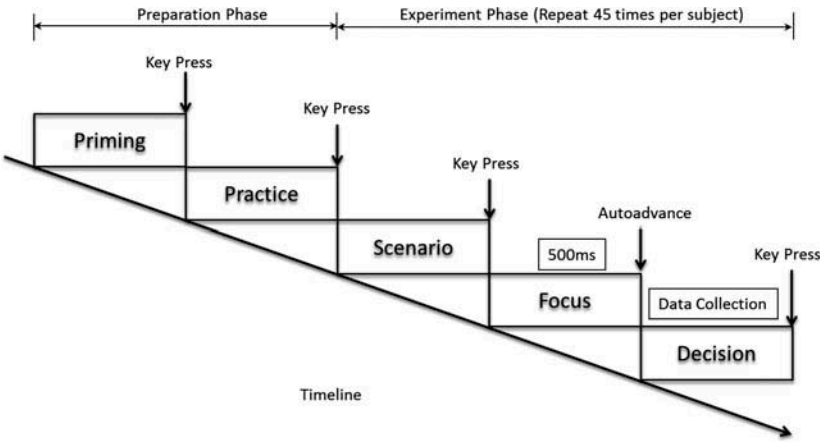

Figure 1. The Procedure for Data Collection

Figure 1 illustrates the sequence of events within the task for Study 1 and Study 2. Once an EEG cap was fitted and the system was calibrated, the priming screen was presented first. When the participant pressed the "Next" button, five practice scenarios were presented on the screen, with four decision choices (No—1, Likely no—2, Likely yes—3, Yes—4) following each scenario, in the exact format and style as study scenarios, but involving no information security related decision making. After the five practice trials, the study scenarios were presented. Once a study scenario was presented on-screen, the participant pressed any button on the special key pad to proceed to the decision screen. A 500 ms display of a "+" sign was introduced to fixate the eyes on the center of the screen before the decision screen was presented. There was no time limit on how long the decision screen was displayed. As soon as the participant pressed one of the decision buttons, the next scenario was presented. This process repeated 45 times for each participant and then the experiment was complete. During the experiment, the participants were instructed to rest their fingers on the four response keys to minimize noise introduced by hand movement. The computer displayed a reward amount on the screen and the participant was paid after completing a postexperiment survey.

Electrophysiological Recordings

The electroencephalogram (EEG) (bandpass 0.01–500 Hz, digitized at 2,048 Hz, gain 1,000, 16-bit A/D conversion) was recorded from an array of 65 sintered silver silver-chloride electrodes based on a modified 10–20 system using an Electrode Arrays cap (Electrode Arrays, El Paso, TX). See Figure 2 for an illustration of the electrode placement on the EEG cap. For both Study 1 and Study 2, the electrode impedance was lower than 20 kΩ for all participants. Vertical eye movements were recorded from two additional electrodes placed below the right and left eyes. During

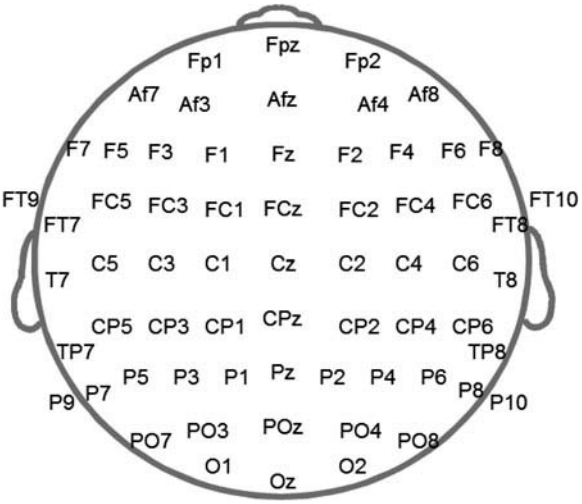

Figure 2. Relative Locations of Electrodes on the Scalp

recording all electrodes were referenced to an electrode placed on the nose [39], and then re-referenced to an average reference for data analysis. The ground electrode was located 10 mm anterior to the medial electrode (Fz). Processing and averaging of the EEG data was done using EMSE 5.3 (Source-Signal Imaging, San Diego). The EEG data were downsampled to 256 Hz and a .1 to 20 Hz zero-phase shift bandpass filter was applied to the data before averaging. Ocular artifacts associated with blinks and saccades were corrected using the Ocular Artifact Correction filter in EMSE. Trials contaminated by other high amplitude artifacts (i.e., ±100 μV) were eliminated during averaging. ERPs were averaged for trials related to control, minor violation, and major violation scenarios from –200 to 2,000 ms around onset of the decision cue.

Partial Least Squares Analysis

The novelty of the experimental paradigm makes it difficult to formulate precise a priori predictions regarding how the ERPs will vary across space (i.e., specific electrodes) and time for the three types of scenarios. Therefore, we decided to utilize partial least squares (PLS) analysis [36, 41] to analyze the ERP data for the two studies. This approach provides a robust analytic framework that eliminates the need to make somewhat arbitrary post hoc choices related to the electrodes and/or time windows included in the analyses, as would be the case when using measures of peak or mean amplitude at a subset of electrodes or time points [36]. PLS analysis allows one to include data for all conditions, electrodes, time points, and participants in a single analysis that decomposes mean differences in ERP amplitude between task conditions into orthogonal latent variables. Each latent variable provides two

pieces of information that are used to identify the effects of the task design and/or group membership on neural activity: (1) the brain scores represent linear contrasts between conditions that express main effect (i.e., Study 1 or 2) or interactions when there is a factorial design (i.e., Study 2); and (2) the electrode saliences represent the distribution of the effect expressed in the brain-score contrasts across electrodes and time points. Bootstrap resampling was used to provide an inferential test of the significance of the brain-score contrast by examining the 95 percent confidence intervals from the bootstrap resampling, and to determine whether the electrode saliences were different from zero by examining the bootstrap ratio. The Normalized Minimum Norm was used to visualize the distribution of the cortical generators of the ERP components captured in the electrode saliences of the latent variables from the PLS analysis.

The PLS analysis included the ERPs from 0 to 2,000 ms after onset of the decision cue at 65 electrodes excluding the two ocular electrodes, and 500 bootstrap samples were used for inferential tests of the brain scores and electrode saliences. Three pieces of information derived from the PLS analysis were used to examine differences in neural recruitment between the three types of scenarios. First, the brain scores represent orthogonal contrasts that characterize the nature of the differences in ERP activity between the three scenarios and are plotted with the 95 percent confidence interval derived from the bootstrap resampling. The individual brain scores express the strength of the effect that is captured by the latent variable for the three types of scenarios. Second, the electrode saliences represent the spatial-temporal distribution of the contrasts in the brain scores. And third, the bootstrap ratio ($\geq$2.0) was used to identify time points that differ from zero. The Normalized Minimum Norm function in the Cortical Current Density Dialog of EMSE 5.3 (Source Signal Imaging, San Diego) was used to estimate the cortical sources of the ERP activity expressed in the electrode saliences of the latent variables from the PLS analysis. The sources were then projected on a generic model of the cortex based on the Montreal Neurological Institute brain for visualization (Source Signal Imaging, San Diego).

Results

Study 1—Validation of Research Paradigm

The primary objective of Study 1 was to validate a paradigm to ensure that (1) measureable ERP data are generated from test participants using information security scenarios as stimuli; and (2) ERP waveforms from the three categories of scenarios are distinguishable and the differences in amplitude between categories are statistically significant at key electrodes relevant to the behavioral theories of the study. Twenty-one participants, as described earlier, participated in the study, and EEG data were recorded using the procedures and parameters described in the previous section.

Table 2. Behavioral Data of Study 1

		Conditions		
Behavioral data	Statistics	Control	Minor	Major
Choice	Mean	2.70	1.66	1.43
	SD	.31	.51	.42
Response time	Mean	7.92	8.07	7.67
	SD	.39	.34	.47

Notes: Choice options are: 1—no; 2—likely no; 3—likely yes; and 4—yes. Response time is in log-transformed milliseconds after onset of stimuli for choice.

Behavioral Data

The average value of decision choices and log-transformed response time for the control, minor violation, and major violation scenarios are presented in Table 2. Response time was log transformed to reduce the influence of particularly slow participants that would result in inflation of the between-participant variability [18]. The mean value of choice for the control scenarios (2.70) was centered at the middle of the scale, indicating that there was not a response bias related to these items. The data show that the mean choice value for minor violations (1.66) was higher than for major violations (1.43), $t(21) = 3.68$, $p < .001$, indicating that participants were sensitive to variation in the severity of the violations represented by the two types of scenarios. The mean value of the log response time was longer for minor violations (8.07) than for major violations (7.67), $t(21) = 7.03$, $p < .001$, indicating that participants may have given greater consideration to the minor violations.

The behavioral results of Study 1 have both expected and unexpected outcomes. We expected that the majority of the participants would be indifferent toward control scenario choices and would reject the minor policy violation choices and strongly reject the major ones, and the mean choices indeed confirm this. On the other hand, we expected that the majority of the participants would take increasingly more time to evaluate and contemplate the choices in the control, minor violation, and major violation scenarios. It turned out that the participants indeed took a longer time to evaluate the choices for minor violations, but quickly rejected the major violation choices. In retrospect, this is in fact sensible because the major violations are so out of the behavioral norm of the majority that the general population would find it objectionable with little contemplation.

ERP Data

After the voltage artifact threshold (i.e., ±100 μV) was applied to remove outliers, the average number of trials contributing to the ERP averages for the outcomes was:

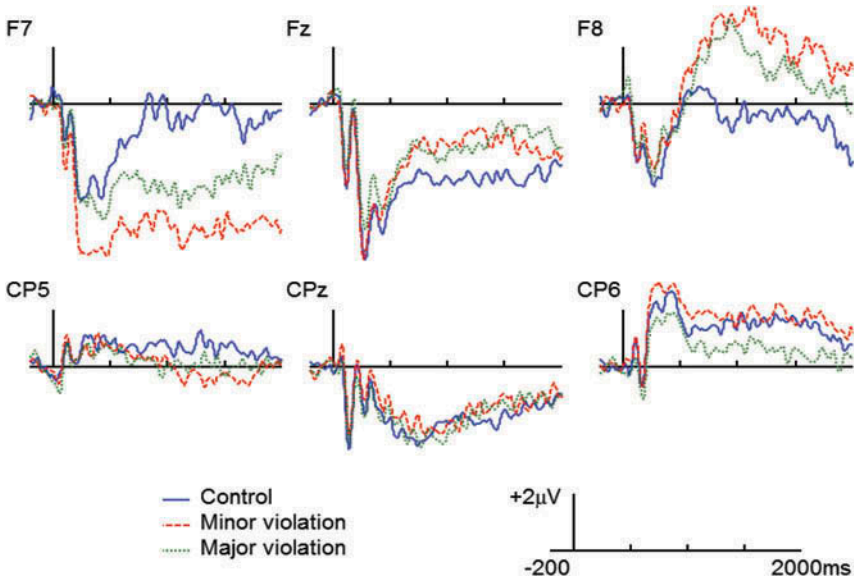

Figure 3. Grand-Averaged ERPs at Six Electrodes Locked to Onset of the Decision Cue for Control, Minor Violation, and Major Violation Scenarios for Study 1

Note: Positive is plotted up, the tall bars represent onset of the decision cue, and the short bars represent 500 ms increments.

control $M = 13.64$, $SD = 1.33$, minor violation $M = 13.59$, $SD = 1.82$, and major violation $M = 13.59$, $SD = 2.17$. The grand-averaged ERPs at a subset of the electrodes are portrayed in Figure 3. These data reveal differences in ERP amplitude between the control, minor violation, and major violation scenarios beginning around 200 ms after onset of the decision cue that persisted for the next several hundred milliseconds. Differences between the ERPs for the three conditions were localized to the lateral (electrodes F7 and F8) and medial (electrode Fz) frontal regions, and the right parietal (electrode CP6) region. These findings are consistent with the literature reviewed in the introduction wherein self-control and decision making were associated with recruitment of the structures within the lateral and medial PFC.

Two latent variables from the PLS analysis were considered. The brain scores for the first latent variable represented a contrast between the minor violation and control scenarios, while the major violation scenarios did not appear to contribute to this contrast since the confidence interval for the brain included zero (see Table 3 and Figure 4). This latent variable accounted for 73.66 percent of the covariance between the scenarios and captured the slow wave activity over lateral and medial frontal regions. The electrode saliences revealed a sustained negativity extending from the left lateral frontal region to the left temporal region, and a sustained positivity extending from the medial frontal region to the right lateral frontal region that significantly differed from zero over much of the analyzed epoch given the results of the bootstrap test. The distributed source analysis of the first latent variable

Table 3. Brain Scores and 95 Percent Confidence Intervals (CI) of Study 1

		Stimuli category		
Latent variable (LV)	Statistics	Control	Minor	Major
LV#1	Brain score	–119	109	10
	95% CI	[–99, –194]	[90, 164]	[–33, 65]
LV#2	Brain score	84	44	–78
	95% CI	[–6, 120]	[–1, 115]	[–79, –139]

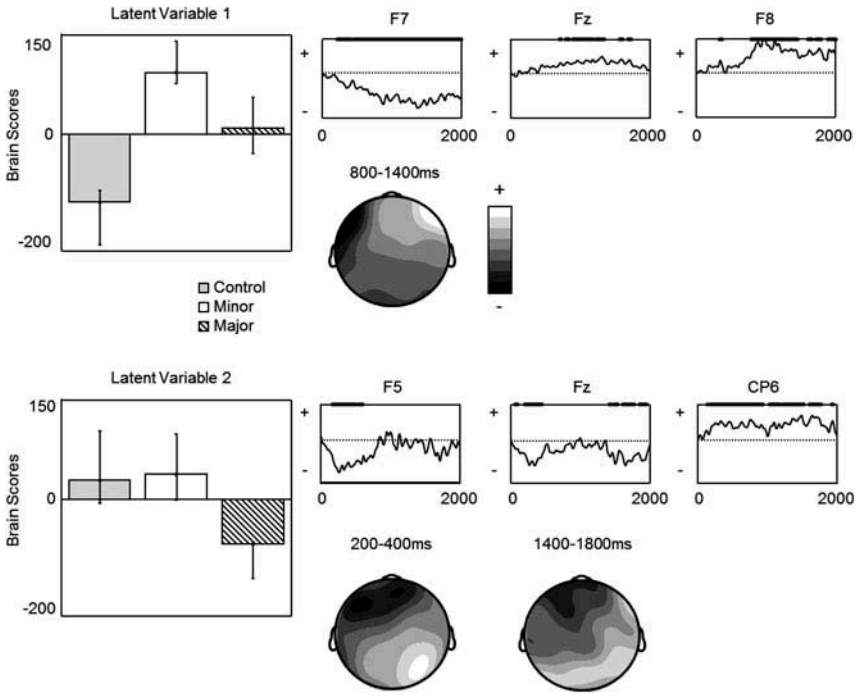

Figure 4. Brain Scores, Electrode Saliences for Three Electrodes and 2D Topography Maps Averaged Across the Interval Reported Above the Map from the PLS Analysis for Study 1

Note: The 95 percent confidence intervals based on the bootstrap resampling are plotted for the brain scores, the "o" above the electrode saliences (shown as solid bands at the top of the waveforms due to overlaps) represents time points where the bootstrap ratio was ≥ 2.0.

revealed that considering minor violation scenarios relative to control scenarios was associated with recruitment of the left inferior frontal and anterior temporal regions, in addition to bilateral activity in the frontal polar region (Figure 5). These findings are consistent with the expectation that the risky decisions represented in the information security violations would be associated with recruitment of neural activity primarily in the prefrontal cortex of the brain.

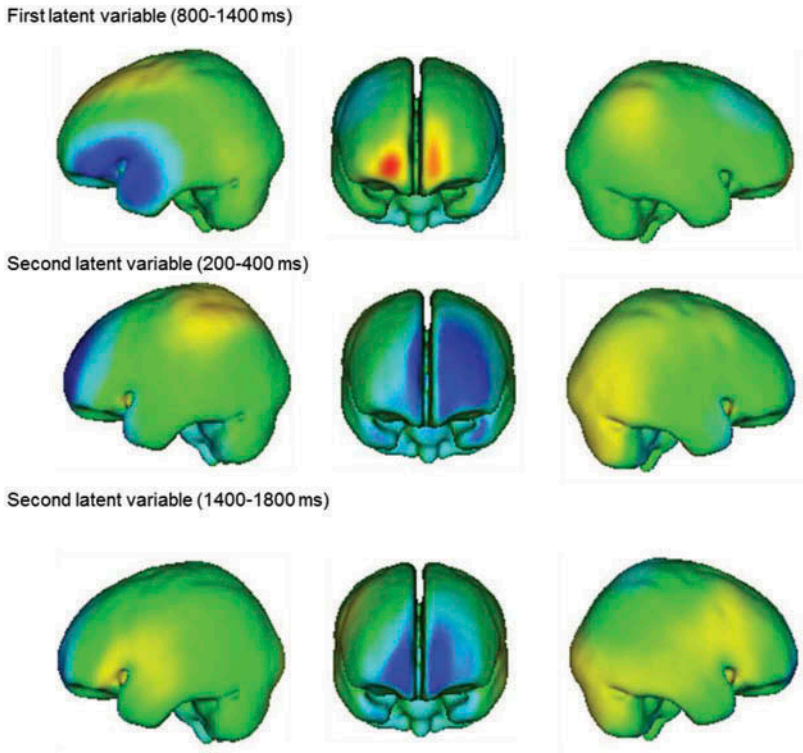

Figure 5. Results of a Distributed Source Analysis Using the Minimum Norm Procedure in EMSE 4.3

Note: Performed on the electrode saliences for the first and second latent variables from the PLS analysis for the intervals represented in the topography maps in Figure 4.

The second latent variable represented a contrast between major violation scenarios and control and minor violation scenarios where the 95 percent confidence interval for the control and minor violation scenarios included zero (see Table 3 and Figure 4). This latent variable accounted for 26.34 percent of the covariance between conditions. The electrode saliences for this latent variable revealed a negativity over the left and midline frontal region (electrodes F5 and Fz) between 100–400 ms and 1,400–1,800 ms after onset of the decision cue, and sustained activity over the right hemisphere extending from the central to the parietal region (electrode CP6) over much of the analyzed epoch (200–1,800 ms). The distributed source analysis of this component revealed that considering major violation scenarios relative to control or minor violation scenarios was associated with recruitment of the left lateral frontal cortex early in the epoch, and bilateral recruitment of the frontal polar region later in the epoch (see Figure 5). Together the results related to the two latent variables reveal that the deliberation of major and minor violations may be associated with the recruitment of distinct regions within the prefrontal cortex.

The results of Study 1 demonstrate that neural activity elicited during the consideration of the minor and major violations of information security policies differs from that elicited during consideration of the control scenarios. Also, these results lead to the suggestion that neural recruitment differs when individuals are faced with decisions that reflect minor or major violations. Relative to control scenarios, both minor and major violations were associated with bilateral recruitment of the frontal polar cortex. In addition, the locus of recruitment within the left lateral frontal cortex appeared to differ between minor (i.e., inferior frontal cortex and anterior temporal cortex) and major (i.e., left medial frontal cortex violations). The results of the distributed source analysis converge with evidence considered in the introduction that also reveals recruitment of the anterior and lateral frontal cortex during risky decision making.

Study 2—The Influence of Self-Control

The primary objective of Study 2 was to investigate the effect of individual differences in self-control on the neural correlates of decision making related to violations of information security policy. We wanted to test whether the low-self-control individuals tend to act faster in selecting a choice and to make riskier decisions that have near-term reward but long-term negative consequences, and whether they tend to recruit different neural circuitry or evoke lower levels of neural activity in contrast to the high-self-control individuals when making decisions related to information security policy violations. For this study, we recruited 40 participants from the participant pool described earlier, based on their scores on the scale of Grasmick et al. [20] (see Appendix A), with 20 from the top 25 percent as low-self-control participants, and 20 from the bottom 25 percent as high-self-control participants. The rest of the test procedures are the same as those used in Study 1.

Behavioral Data

The average value of decision choices and log-response time for the control, minor violation, and major violation scenarios for the high- and the low-self-control groups are reported in Tables 4 and 5. The mean value of choice for the control scenarios was centered at the middle of the scale and was similar in the two groups (2.76 for high self-control, and 2.75 for low self-control), $t(38) = .11$, $p = .92$, and the low-self-control individuals responded more quickly than high-self-control individuals to control scenarios (7.71 vs. 7.93), $t(38) = 2.56$, $p < .02$. The mean value of choice for minor violations is significantly higher than that for major violations, $F(1,38) = 23.80$, $p < .001$; the mean values of choice of the low-self-control group were higher for both the minor and major violations than those of the high-self-control group, although this difference was not significant: main effect of group $F(1,38) = 1.30$, $p = .26$, group × violation interaction $F(1,38) = 1.97$, $p = .17$. Response time was

Table 4. Behavioral Intention by Stimuli Type and Self-Control Group of Study 2

		Behavioral intention choice ANOVA					
Stimuli category	Self-control group	Mean	SD	Mean	SD	*t*-value	*p* (two-tailed)
Control	H	2.76	.39	2.76	.54	–.06	.967
	L			2.75	.46		
Minor	H	1.47	.39	1.38	.26	1.86	.07
	L			1.55	.25		
Major	H	1.32	.37	1.27	.17	1.18	.256
	L			1.37	.24		

Note: Choice options are: 1—no; 2—likely no; 3—likely yes; and 4—yes.

Table 5. Response Time by Stimuli Type and Self-Control Group of Study 2

		Response Time ANOVA					
Stimuli category	Self-control group	Mean	SD	Mean	SD	*t*	*p* (two-tailed)
Control	H	7.82	.29	7.93	.27	2.60	.01
	L			7.71	.26		
Minor	H	7.79	.40	7.83	.42	.75	.46
	L			7.74	.37		
Major	H	7.61	.37	7.74	.39	2.25	.03
	L			7.48	.32		

Note: Response time is in log-transformed milliseconds after onset of stimuli for choice.

longer for minor violations than for major violations, $F(1,38) = 19.48$, $p < .001$. There was a marginally significant interaction between group and violation type for response time, $F(1,38) = 3.94$, $p = .054$, reflecting faster response time for the low-self-control group than for the high–self-control group for major violations, but not for minor violations. The main effect of group on response time was not significant, $F(1,38) = 2.38$, $p = .13$.

We can see that Hypothesis 1, which stipulates that individuals with low self-control tend to choose actions with near-term gain but potential long-term loss in contrast to those with high self-control, is not supported; and Hypothesis 2, which stipulates that individuals with low self-control tend to make choices faster in contrast to those with high self-control, is partially supported by the behavioral data. Although the low-self-control participants indeed have higher mean values for their choices, thus more risk intention, than the high-self-control individuals in both minor and major violation conditions, the differences are not statistically significant at $p < 0.05$ level. However, a bit of caution must be exercised here before we dismiss Hypothesis 1. Since the behavior intention choice was completely under the control

of the participants, social desirability bias [47] was real and posed a significant threat to the true intention of the participants, even with the deceptive design as described before. It is entirely possible that this social desirability bias in both participant groups masked the true behavioral intention and rendered it nonsignificant when comparing between the two groups. Unfortunately, there is no reliable method we can use to tease out this bias and reveal the true intentions of the participants.

On the other hand, the response-time difference between the high- and low-self-control participants in the control and major violation conditions are indeed significant at $p < 0.05$ level, but not significant in the minor violation condition. Therefore, the high-self-control participants indeed took more time than the low-self-control individuals in contemplating the scenarios that severely violate information security policies of the organization and could have significant long-term negative consequences before making a choice similar to that of the low-self-control participants. We have more confidence in the truthfulness of response time because it is less likely subject to social desirability or other common method biases as identified by Podsakoff et al. [47].

ERP Data

The average number of trials contributing to the ERP averages for the outcomes was slightly lower than 15 after a few trials were removed for not meeting the voltage threshold (±100 μV): high self-control control $M = 14.70$, $SD = .47$, minor violation $M = 14.35$, $SD = 1.14$, and major violation $M = 14.65$, $SD = .81$; low self-control control $M = 14.35$, $SD = 1.79$, minor violation $M = 14.55$, $SD = 1.57$, and major violation $M = 14.15$, $SD = 2.46$. The grand-averaged ERPs at a subset of the electrodes for Study 2 are portrayed in Figure 6. These data reveal differences in the amplitude of the ERPs between the high- and low-self-control groups for the control, minor violation, and major violation scenarios over the frontal and posterior regions of the scalp. In the high-self-control individuals, differences in ERP amplitude for the three scenarios are similar to those observed in Study 1, with the ERPs for the minor and major violation scenarios being more negative over the left frontal region and more positive over the right frontal region than the ERPs for the control scenarios. In contrast, for the low-self-control individuals, this general pattern was reversed with the ERPs for control scenarios being more negative over the left hemisphere and more positive over the right hemisphere than for minor or major violation scenarios. These observations provide qualitative support for Hypothesis 3 by demonstrating differences in neural recruitment over the frontal region of the scalp in low-self-control participants relative to high-self-control participants in the context of information security policy violations.

PLS and distributed-source analysis of the ERP data provide further insights into the locus of differences in neural recruitment related to variation in self-control. Once again, two latent variables were examined. As in Study 1, the first latent variable from the PLS analysis represented a contrast between minor violation and

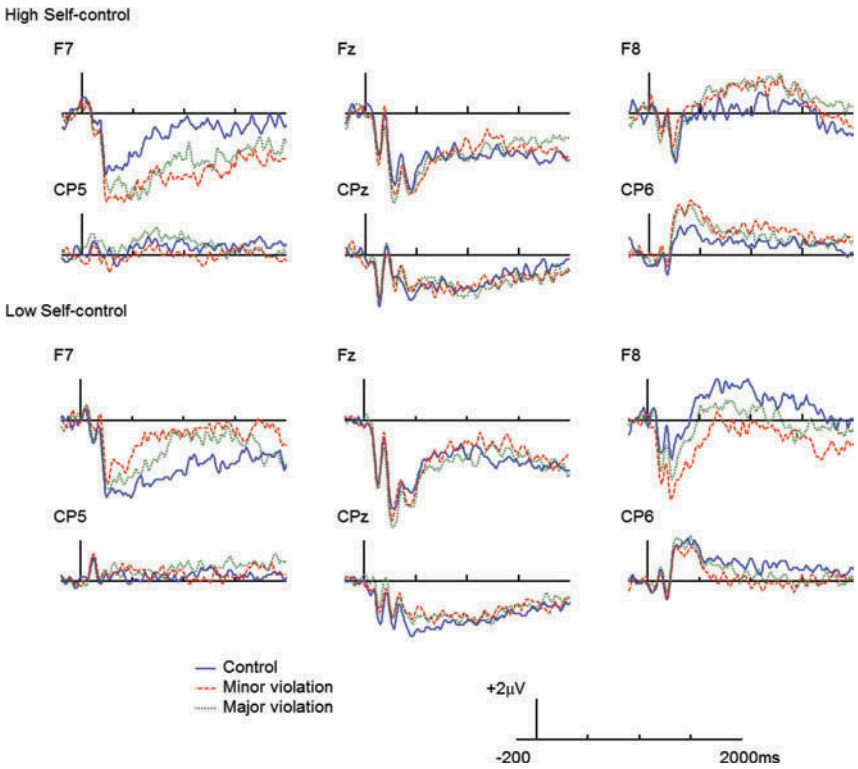

Figure 6. Grand-Averaged ERPs at Six Electrodes for the High and Low Self-Control Groups Locked to Onset of the Decision Cue for Control, Minor Violation and Major Violation Scenarios for Study 2

Note: Positive is plotted up, the tall bars represent onset of the decision cue, and the short bars represent 500 ms increments.

control scenarios that captured the reversal of the ordering of the ERPs over the left and right frontal regions between the two groups (see Table 6 and Figure 7), and accounted for 49.57 percent of the covariance between conditions. For the high-self-control group, the pattern of brain scores was similar to Study 1, while the contrast

Table 6. Brain Scores and 95% Confidence Intervals (CI) of Study 2

		Low self-control			High self-control		
Latent variable	Statistics	Control	Minor	Major	Control	Minor	Major
LV#1	Brain score	76	–77	.43	–50	35	16
	95% CI	[55, 126]	[–58, –123]	[–30, 30]	[–26, –104]	[.57, 87]	[–11, 55]
LV#2	Brain score	28	–10	–19	47	10	57
	95% CI	[5, 78]	[–40, 15]	[–4, –45]	[41, 100]	[–15, 40]	[–53, 120]

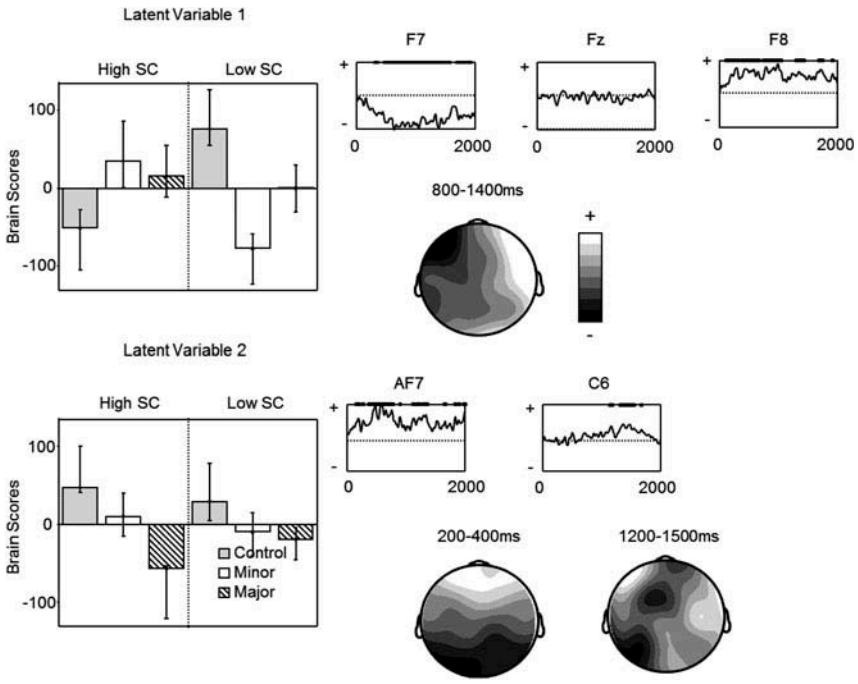

Figure 7. Brain Scores, Electrode Saliences for Three Electrodes and 2D Topography Maps Averaged Across the Interval Reported Above the Map from the PLS Analysis for Study 2

Note: The 95 percent confidence interval based upon the bootstrap resampling is plotted for the brain scores, the "o" above the electrode saliences (shown as solid bands at the top of the waveforms due to overlaps) represent time points were the bootstrap ratio was ≥ 2.0 for the first latent variable and ≥ 1.75 for the second latent variable.

was reversed in the low-self-control group. Consistent with the results of Study 1, the electrode saliences for the first latent variable represented a sustained negativity over the left lateral frontal region and a sustained positivity over the right lateral frontal region, and the bootstrap test indicated that both of these modulations differed from zero over much of the epoch. In contrast to the first latent variable in Study 1, the medial frontal region did not appear to contribute to the first latent variable in Study 2. The distributed-source analysis of this component revealed that the consideration of minor violation scenarios relative to control scenarios was associated with recruitment of the right and left inferior frontal cortex and anterior temporal cortex (Figure 8).

These findings partially support Hypothesis 3 by revealing differences in neural recruitment in the right lateral frontal region in low- versus high-self-control individuals when considering minor violations of information security policies. These data also reveal that the effect of self-control extends to the left lateral frontal region. Interestingly, the effect of self-control for the right and left lateral frontal regions reflected differential neural recruitment in the low- and high-self-control individuals rather than simply a reduction in neural recruitment in the low-self-control

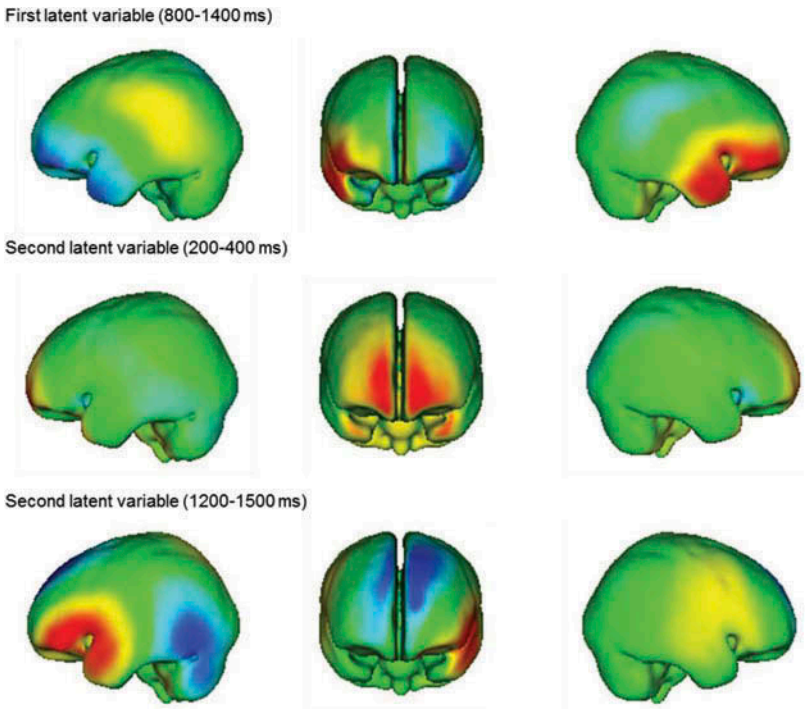

Figure 8. Results of a Distributed Source Analysis Using the Minimum Norm Procedure in EMSE 4.3 Performed on the electrode saliences for the first and second latent variables from the PLS analysis for the intervals represented in the topography maps in Figure 7.

individuals. This finding may indicate that individuals with low and high self-control approach the deliberation of minor violations of security policies somewhat differently.

The second latent variable from the PLS analysis represented a contrast between the major violation and control scenarios (Figure 7) and accounted for 21.58 percent of the covariance between conditions. The nature of the contrast was similar for the high- and low-self-control groups, and the contrast was weaker in the low-self-control group than in the high-self-control group. The bootstrap test revealed that the electrode saliences were different from zero between 200–400 ms and 1,600–1,800 ms over the midline frontal region, between 200–400 ms over the right parietal region, and between 1,100–1,600 ms over the right temporal region. The distributed source analysis of this component revealed that the consideration of major violations relative to control scenarios was associated with recruitment of the bilateral frontal polar region between 200 ms and 400 ms and recruitment of the left medial and inferior frontal and right lateral frontal regions between 1,200 ms and 1,500 ms. These findings support Hypothesis 3 by revealing a reduction in neural recruitment within the right PFC in individuals with low self-control relative to those with high self-control when considering major violations of information security policy. In

addition, the reduction in neural recruitment in individuals with low self-control extended to the left PFC as well as the posterior cortical structures.

The PLS analysis revealed both qualitative (latent variable 1) and quantitative (latent variable 2) differences in neural recruitment between individuals with high or low self-control related to the recruitment of lateral and medial frontal cortex. The first latent variable revealed a disassociation between high-self-control individuals and low-self-control individual. The distribution of this effect over the lateral frontal region and localization of the effect to the inferior frontal cortex are consistent with the prediction that recruitment of the inferior frontal cortex is associated with self-control. The reversal of the effect between the two groups and the similarity of the effect in high-self-control individuals and the nonspecific participants in Study 1 suggests that low-self-control individuals may approach the deliberation of minor violations of information security policy somewhat differently than do other individuals. The second latent variable revealed a reduction in the strength of the contrast for low-self-control individuals relative to high-self-control individuals. This finding may indicate that low- and high-self-control individuals utilize similar processing when deliberating over major violations, but that low-self-control individuals are either less likely to engage these processes or they engage them more superficially than high-self-control individuals. As predicted in Hypothesis 3, underrecruitment was observed in the right hemisphere, including the right PFC, for low-self-control individuals; and interestingly, this effect also extended to the left hemisphere including the left PFC, which has not been reported before in neuroscience-based self-control studies.

Discussion

This study and the main findings presented above have some significant theoretical contributions and interesting practical implications for information security and human decision making in general. Our findings, along with those of other studies using neuroscience methodologies [2, 3, 4, 23, 34, 38, 40] show that the individual characteristic of self-control, as described in Gottfredson and Hirschi [19] and measured by Grasmick et al. [20], is associated with activation within the medial and lateral PFC. This is not a mere confirmation of the findings in prior studies in the area of neuroscience, but a significant step forward in building the foundation for criminology and information security studies that use neuroscience tools. As discussed earlier, the extant studies in neuroscience involving self-control have used a variety of measures not commonly found in the criminology or information security literatures. Our results show that self-control as measured by Grasmick et al. [20] has effects on neural process characteristics similar to the effects of other self-control measures used in neuroscience studies. This evidence lends some support to the idea that self-control is a stable characteristic of an individual, formed early in life, and remains relatively stable throughout the life span [19]. This finding opens an entirely new area of research for criminology and information security scholars who believe

in the central role of self-control in individual behavior, especially in the context of risk taking and decision making.

The second contribution of this study is the development and validation of an ERP paradigm for scenario-based research in the context of information security and human decision making in general. Given the critical role of paradigm in neuroscience research, a validated ERP paradigm enables reliability, continuity, and replicability that much of the survey-based research lacks in social science disciplines. While the paradigm will continue to improve as more researchers use it, a solid foundation has been established for future research using these types of methodologies. In criminology and information security research, due to the unique social and ethical stigma associated with the focal behavior (deviant or criminal), it is mostly infeasible to directly observe the relevant decisions or behavior in either laboratory or field conditions. This is in contrast to most neuroscience studies, which frequently use decision cues directly emulating the focal phenomena in laboratory conditions. The research paradigm developed and validated in our study bridges this significant gap between scenario-based research and neuroscience research, enabling future criminology and information security research to take advantage of neuroscience theories, methodologies, and tools to significantly advance the science of the focal disciplines.

The final contribution of this study is its validation of the Grasmick et al. [20] scale for measuring self-control with neural activity evidence. Given the significance of the self-control construct and its measurement in criminology and information security research, having a psychological instrument that has a neuroscience foundation is a major step forward and establishes a solid foundation for future criminological and information security research in which self-control is a central construct. Our results show that individuals classified using this scale as low- and high-self-control indeed demonstrated significant differences in their behavioral actions and neural activities when contemplating challenging information security decisions. The low-self-control participants tended to make quicker decisions and generated less negative ERPs in the left PFC region and less positive ERPs in the right PFC region than the high-self-control participants did when contemplating minor and major information security violation choices. Although we cannot use EEG signals at specific electrodes to determine the exact location of the neural activity that generated the EEG signals due to the limited spatial accuracy of the EEG measurement, those regions where high-self-control individuals had stronger ERP waves, either positive or negative in magnitude, are consistent with the findings of neuroscience studies using more spatially accurate fMRI tools [2, 3, 23, 38].

Our findings have at least two important practical implications. First, we have shown that the instrument developed by Grasmick et al. [20] is a valid measure of individual self-control. In the literature there are a variety of self-control scales developed by psychologists and criminologists. Our results showed that the individuals identified as having high and low self-control using the Grasmack et al. [20] scale had ERP and behavioral characteristics consistent with those identified by neuroscientists with more sophisticated tools. Given the simple structure and easy

implementation of the Grasmick et al. [20] scale as compared to the neural imaging tools for measuring individual self-control characteristics, this study provides credence for teams and organizations to use the scale for quick screening of individuals in order to determine the best fit of individuals for specific tasks that may or may not require a high level of self-control.

Perhaps the most interesting practical implication of our findings is that self-control screening of employees is not only practical but also recommended for organizations to protect their digital assets. This study confirms that self-control is an individual characteristic attributable to neural structures in the PFC, DLPFC, and/or adjacent regions of the brain. This may dampen the hope of advocates of SETA (security education, training, and awareness) programs (e.g., 8, 11) in terms of effectiveness of these types of programs in information security management. This is because SETA assumes rational decision making by individuals. Given the observation that self-control in adults can be attributed to the recruitment of specific neural processes in the brain that cannot be consciously manipulated, training may do little to alter these neural processes in low-self-control adults. Thus, if low-self-control employees are entrusted with valuable digital assets, the effectiveness of SETA programs in managing internal security threats originating from some of these individuals are questionable at best. However, we do want to caution that employee screening using a psychological instrument for the purpose of job assignment is a sensitive matter that may be subject to ethical and privacy questions and state and federal regulations [37].

As one of the first studies to use neuroscience techniques and methodologies for investigating human decision making in the context of information security, this study inevitably has some limitations. First, the relatively small sample size, coupled with large variances in the ERP data, made the statistical differences in the ERP component between the low- and high-self-control groups less reliable and perhaps less significant than they could be. Future research may attempt to recruit more participants, for example, 40 in each group, to improve the reliability of the data and analyses. Second, accuracy was coarse in localizing ERP data due to the nature of EEG measurement. While we were able to determine the activation of neural processes in the left and right hemispheres after onset of a decision cue, and suggest the possible sources in the prefrontal cortex and lateral frontal regions based on PLS and distributed source analyses, the EEG data cannot pinpoint with the same precision as fMRI the specific locations in the brain where these neural processes occur. Future study may supplement ERP data with fMRI imaging to provide a more refined understanding of and insight into how self-control influences decision making in information security and other social, economic, and criminological contexts. Third, our mechanism for measuring decision time is relatively primitive even with the precaution taken to minimize hand-movement delays. Other factors such as reading speed and eagerness to complete the experiment could have contributed to the time measures in addition to the level of self-control. Future research should incorporate these factors as control variables to calibrate the decision-time measures. Fourth, in order to minimize the effect of sex and age in this exploratory study, our

experiments involved only college-age male participants, and thus the findings of this study may not be applicable to the general population until more studies with various sex and age groups are conducted. Finally, our approach of using group membership rather than direct manipulation of the self-control variable cannot effectively eliminate the effects of other confounding factors, such as emotion and attitude, in the participants on their neural activities when stimuli are onset. Future research should consider more comprehensive prescreening and data collection mechanisms for controlling spurious factors.

Conclusion

In this study, we used ERPs to investigate the neural correlates of human decision and self-control in the context of information security in laboratory settings. Our results point to the neural locus of individual differences in self-control as measured by the Grasmick et al. [20] scale, and reveal that individuals with low and high self-control may activate different neural processes when making decisions related to information security policy violations, and that low-self-control individuals tend to make choices faster than high-self-control individuals do. These results are consistent with neuroscience studies about self-control in various social and economic contexts.

Perhaps more important, this study establishes the validities of two important research instruments: an EEG/ERP paradigm for scenario-based research of decision making in the context of information security, and the Grasmick et al. [20] scale as a valid measure of individual self-control. These two instruments can serve as a foundation for future research that uses neuroscience theories, methodologies, and tools in information security and other social, economic, and criminological studies. In addition, the Grasmick et al. [20] scale can be used by researchers and managers for screening and selecting individuals based on self-control characteristics. Hu et al. [27] have advocated the screening of employees for self-control in order to improve information security in organizations. This study provided further evidence for both the validity of the instrument that can be used for the screening and the scientific foundation for conducting such screening for better information security management, with the caveat that relevant workplace ethical, privacy, and other regulations must be observed.

References

1. Antonaccio, O., and Tittle, C.R. Morality, self-control, and crime. *Criminology*, 46, 2 (2008), 479–510.

2. Aron, A.R.; Robbins, T.W.; and Poldrack, R.A. Inhibition and the right inferior frontal cortex. *TRENDS in Cognitive Sciences*, 8, 4 (2004), 170–177.

3. Bechara, A. Decision making, impulse control, and loss of willpower to resist drugs: A neurocognitive perspective. *Nature Neuroscience*, 8, 11 (2005), 1458–1463.

4. Boes, A.D.; Bechara, A.; Tranel, D.; Anderson, S.W.; Richman, L.; and Nopoulos, P. Right ventromedial prefrontal cortex: A neuroanatomical correlate of impulse control in boys. *Social Cognitive and Affective Neuroscience*, 4, 1 (2009), 1–9.

5. Boudreau, C.; McCubbins, M.D.; and Coulson, S. Knowing when to trust others: An ERP study of decision making after receiving information from unknown people. *SCAN*, 4 (2009), 23–34.

6. Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A.; and Boss, R.W. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18, 2 (2009), 151–164.

7. Brocke, J.V., and Liang, T.P. Guidelines for neuroscience studies in information systems research. *Journal of Management Information Systems*, 30, 4 (2014), 211–234.

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

9. Clark, L.; Manes, F.; Antoun, N.; Sahakian, B.J.; and Robbins, T.W. The contributions of lesion laterality and lesion volume to decision-making impairment following frontal lobe damage. *Neuropsychologia*, 41, 11 (2003), 1474–1483.

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

11. D'Arcy, J.; Havav, A.; and Galletta, D. User Awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20, 1 (2009), 79–98.

12. DeLisi, M.; Hochstetler, A.; Higgins, G.E.; Beaver, K.M.; and Graeve, C.M. Toward a general theory of criminal justice: Low self-control and offender noncompliance. *Criminal Justice Review*, 33, 2 (2008), 141–158.

13. Dimoka, A. What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly*, 34, 2 (2010), 373–396.

14. Dimoka, A.; Pavlou, P.A.; and Davis, F. NeuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research*, 22, 4 (2011), 687–702.

15. Duckworth, A.L., and Kern, M.L. A meta-analysis of the convergent validity of self-control measures. *Journal of Research in Personality*, 45, 3 (2011), 259–268.

16. Duncan, J., and Owen, A.M. Common regions of the human frontal lobe recruited by diverse cognitive demands. *Trends in Neurosciences*, 23, 10 (2000), 475–483.

17. Ernst & Young. Borderless Security: Ernst & Young 2010 Global Information Security Survey. 2010. Available at http://www.ey.com/Publication/vwLUAssets/Global_information_security_survey_2010_advisory/$FILE/GISS%20report_final.pdf.

18. Faust, M.E.; Balota, D.S.; Spieler, D.H.; and Ferraro, F.R. Individual differences in information- processing rate and amount: Implications for group differences in response latency. *Psychological Bulletin*, 125, 6 (1999), 777–799.

19. Gottfredson, M., and Hirschi, T. *A General Theory of Crime*. Stanford, CA: Stanford University Press, 1990.

20. Grasmick, H.; Tittle, G.; Bursik Jr., R.; and Arneklev, B. Testing the core implications of Gettfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency*, 30, 1 (1993), 5–29.

21. Gregor, S.; Lin, A.C.H.; Gedeon, T.; Riaz, A.; and Zhu, D. Neuroscience and a nomological network for the understanding and assessment of emotions in information systems research. *Journal of Management Information Systems*, 30, 4 (2014), 13–48.

22. de Guinea, A.O.; Titah, R.; and Léger, P.-M. Explicit and implicit antecedents of users' behavioral beliefs in information systems: A neuropsychological investigation. *Journal of Management Information Systems*, 30, 4 (2014), 179–210.

23. Hare, T.A.; Camerer, C.F.; and Rangel, A. Self-control in decision-making involves modulation of the vmPFC valuation system. *Science*, 324, 5927 (2009), 646–648.

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

25. Heatherton, T.F.; Peter, C.; Polivy, J.; King, G.A.; and McGree, S.T. The (mis)measurement of restraint: An analysis of conceptual and psychometric issues. *Journal of Abnormal Psychology*, 97, 1 (1988), 19–28.

26. Higgins, G.E.; Wilson, A.L.; and Fell, B.D. An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture*, 12, 3 (2005), 166–184.

27. Hu Q.; Xu, Z.C.; Dinev, T.; and Ling, H. Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54, 6 (2011), 34–40.

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

29. Hu, Q.; Xu, Z.C.; and Yayla, A. Why college students commit computer hacks: Insights from a cross culture analysis. *Proceedings of the Seventeenth Pacific Asia Conference on Information Systems*, Jeju, South Korea, June 18–22, 2013.

30. Inzlicht, M., and Gutsell, J.N. Running on empty: Neural signals for self-control failure. *Psychological Science*, 18, 11 (2007), 933–937.

31. Jimura, K.; Chushak, M.S.; and Braver, T.S. Impulsivity and self-control during intertemporal decision making linked to the neural dynamics of reward value representation. *Journal of Neuroscience*, 33, 1 (2013), 344–357.

32. Johnston, A.C., and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 33, 4 (2010), 549–566.

33. Kanfer, F.H., and Goldfoot, D.A. Self-control and tolerance for noxious stimulation. *Psychological Report*, 18 (1966), 79–85.

34. Knoch, D., and Fehr, E. Resisting the power of temptations: The right prefrontal cortex and self-control. *Annals of the New York Academy of Sciences*, 1104, 1 (2007), 123–134.

35. Kuan, K.K.Y.; Zhong, Y.; and Chau, P.Y.K. Informational and normative social influence in group-buying: Evidence from self-reported and EEG data. *Journal of Management Information Systems*, 30, 4 (2014), 151–178.

36. Lobaugh, N.J.; West, R.; and McIntosh, A.R. Spatiotemporal analysis of experimental differences in event-related potential data with partial least squares. *Psychophysiology*, 38, 3 (2001), 517–530.

37. London, M., and Bray, D.W. Ethical issues in testing and evaluation for personnel decisions. *American Psychologist*, 35, 10 (1980), 890–901.

38. Lopez, R.B.; Hofmann, W.; Wagner, D.D.; Kelley, W.M.; and Heatherton, T.F. Neural predictors of giving in to temptation in daily life. *Psychological Science*, 25, 7 (2014), 1337–1344.

39. Luck, S.J. *An Introduction to the Event-Related Potential Technique*. Cambridge, MA: MIT Press, 2005.

40. Martin, L.E., and Potts, G.F. Impulsivity in decision-making: An event-related potential investigation. *Personality and Individual Differences*, 46, 3 (2009), 303–308.

41. McIntosh, A.R., and Lobaugh, N.J. Partial least squares analysis of neuroimaging data: Applications and advances. *NeuroImage*, 23, S1 (2004), S250–S263.

42. Minas, R.K.; Potter, R.F.; Dennis, A.R.; Bartelt, V.; and Bae, S. Putting on the thinking cap: Using NeuroIS to understand information processing biases in virtual teams. *Journal of Management Information Systems*, 30, 4 (2014), 49–82.

43. Miller, E.K., and Cohen, J.D. An integrative theory of prefrontal cortex function. *Annual Review of Neuroscience*, 24 (2001), 167–202.

44. Muraven, M., and Baumeister, R.F. Self-regulation and depletion of limited resources: Does self-control resemble a muscle? *Psychological Bulletin*, 126, 2 (2000), 247–259.

45. Patton, J.H.; Stanford, M.S.; and Barratt, E.S. Factor structure of the Barratt impulsiveness scale. *Journal of Clinical Psychology*, 51, 6 (1995), 768–774.

46. Piquero, A., and Tibbetts, S. Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly*, 13, 3 (1996), 481–510.

47. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; and Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88, 5 (2003), 879–903.

48. Riedl, R.; Banker, R.D.; Benbasat, I.; Davis, F.D.; Dennis, A.R.; Dimoka, A.; Gefen, D.; Gupta, A.; Ischebeck, A.; Kenning, P.; Gernot, M.-P.; Pavlou, P.A.; Straub, D.W.; vom Brocke, J.; and Weber, B. On the foundations of NeuroIS: Reflections on the Gmunden Retreat 2009. *Communications of the Association for Information Systems*, 27, 15 (2010), 243–264.

49. Riedl, R.; Mohr, P.N.C.; Kenning, P.H.; Davis, F.D.; and Heekeren, H.R. Trusting humans and avatars: A brain imaging study based on evolution theory. *Journal of Management Information Systems*, 30, 4 (2014), 83–114.

50. Schoepfer, A., and Piquero, A.R. Self-control, moral beliefs, and criminal activity. *Deviant Behavior*, 27, 1 (2006), 51–71.

51. Seipel, C., and Eifler, S. Opportunities, rational choice, and self-control: On the interaction of person and situation in a general theory of crime. *Crime and Delinquency*, 56, 2 (2010), 167–197.

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

53. Straub, D.W. Effective IS security: An empirical study. *Information Systems Research*, 1, 3 (1990), 255–276.

54. Tranel, D.; Bechara, A.; and Denburg, N.L. Asymmetric functional roles of right and left ventromedial prefrontal cortices in social conduct, decision-making, and emotional processing. *Cortex*, 38, 4 (2002), 589–612.

55. Vance, A.; Anderson, B.; Kirwan, B.; and Eargle, D. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems Research*, 15, 10(2014), 679–722.

56. Vazsonyi, A.T.; Pickering, L.E.; Junger, M.; and Hessing, D. An empirical test of a general theory of crime: A four nation comparative study of self-control and the prediction of deviance. *Journal of Research in Crime and Delinquency*, 38, 2 (2001), 91–131.

57. Wikström, P.O.H., and Svensson, R. When does self-control matter? The interaction between morality and self-control in crime causation. *European Journal of Criminology*, 7, 5 (2010), 395–410.

58. Wright, B.R.E.; Caspi, A.; Moffitt, T.E.; and Paternoster, R. Does the perceived risk of punishment deter criminally prone individuals? Rational choice, self-control, and crime. *Journal of Research in Crime and Delinquency*, 41, 2 (2004), 180–213.

59. Xu, Z.C.; Hu, Q.; and Zhang, C.H. Why computer talents become computer hackers. *Communications of the ACM*, 56, 4 (2013), 64–74.

60. Zhang, L.; Smith, W.W.; and McDowell, W.C. Examining digital piracy: Self-control, punishment, and self-efficacy. *Information Resources Management Journal*, *22*, 1 (2009), 24–44.

Appendix A

Pre-Test and Self-Control Screening Survey

Section I: Respondent profile (choose one)

Age	• 19 • 20 • 21 • 22 • > 22 (Specify: _____)	Class	• Freshman • Sophomore • Junior • Senior
Sex	• Male • Female	GPA	• 2.0–2.5 • 2.6–2.9 • 3.0–3.5 • 3.6–4.0
Major	• Accounting • Finance • Marketing • Management • MIS • SCM • Other _____	Organizational experience	• Full-time employee • Part-time employee • Student internship • Never worked
Computer skills	• Personal use only • Microsoft Office skills • Programming • Hardware and software • Advanced knowledge	Average hours of using computers per day	• <3 (Specify: _____) • 3 • 4 • 5 • > 6 (Specify: _____)

Section II: Self-control (adapted from [20])

1—Strongly disagree	4—Neutral	7—Strongly agree

IP1	I often act on the spur of the moment without stopping to think.	1 2 3 4 5 6 7
IP2	I don't devote much thought and effort to preparing for the future.	1 2 3 4 5 6 7
IP3	I often do whatever brings me pleasure here and now, even at the cost of some distant goal.	1 2 3 4 5 6 7
IP4	I'm more concerned with what happens to me in the short run than in the long run.	1 2 3 4 5 6 7
RS1	I like to test myself every now and then by doing something a little risky.	1 2 3 4 5 6 7
RS2	Sometimes I will take a risk just for the fun of it.	1 2 3 4 5 6 7
RS3	I sometimes find it exciting to do things for which I might get in trouble.	1 2 3 4 5 6 7
RS4	Excitement and adventure are more important to me than security.	1 2 3 4 5 6 7
SC1	I try to look out for myself first, even if it means making things difficult for other people.	1 2 3 4 5 6 7
SC2	I have little sympathy for other people when they are having problems.	1 2 3 4 5 6 7

(continues)

Appendix A. Continued

Section II: Self-control (adapted from [20])		
SC3	If things I do upset people, it's their problem not mine.	1 2 3 4 5 6 7
SC4	I will try to get the things I want even when I know it's causing problems for other people.	1 2 3 4 5 6 7
ST1	I frequently avoid projects that I know will be difficult.	1 2 3 4 5 6 7
ST2	When things get complicated, I tend to quit and withdraw.	1 2 3 4 5 6 7
ST3	The things in life that are easiest to do bring me the most pleasure.	1 2 3 4 5 6 7
ST4	I dislike really hard tasks that stretch my abilities to the limit.	1 2 3 4 5 6 7
PA1	If I had a choice, I would almost always rather do something physical than something mental.	1 2 3 4 5 6 7
PA2	I almost always feel better when I am on the move than when I am sitting and thinking.	1 2 3 4 5 6 7
PA3	I like to get out and do things more than I like to read or contemplate ideas.	1 2 3 4 5 6 7
PA4	I seem to have more energy and a greater need for activity than most other people my age.	1 2 3 4 5 6 7
TP1	I lose my temper pretty easily.	1 2 3 4 5 6 7
TP2	Often when I am angry at people I feel more like hurting them than talking to them about why I am angry.	1 2 3 4 5 6 7
TP3	When I am really angry, other people had better stay away from me.	1 2 3 4 5 6 7
TP4	When I have a serious disagreement with someone, it is usually hard for me to talk calmly about it without getting upset.	1 2 3 4 5 6 7

Key: IP—Impulsivity, RS—Risk taking, SC—Self-centered, ST—Simple task, PA—Physical activities, TP—Tempe

Appendix B

Scenarios and Stimuli for EEG/ERP Study of Information Security Policy Violations

1. Purpose

These test scenarios are designed to validate a research design paradigm for an ERP study regarding individual differences in information security policy violation behavior. If validated, these test scenarios and the associated paradigm will be used to test research hypotheses in the same context.

2. Design Philosophy

In order to test different neurological and neurophysiological responses to different decision-making scenarios, this validation test requires a collection of 45 test scenarios, evenly split between control, minor, and major information security policy violation decisions. Each test participant will be presented with all 45 scenarios in an identical pseudo-random order predetermined by the researchers.

3. Test Scenarios

3.0 Priming Messages

Type	Message	Purpose
Motivating message	Based on your answers to the previous survey, the computer has established a psychological profile about your most likely behavior under various circumstances. When participating in this experiment, the closer your answers reflect the predicated behavior, the more money you will earn. You could earn $15–$25 depending on your answers. The best strategy to earn more money is to be as truthful as possible. The computer will calculate the payout at the end of the experiment and display that amount to you.	To motivate participants to be truthful in their responses
Opening Message	Josh works for the IT department of a large global manufacturing company that supplies sophisticated electronic control instruments for civilian and military uses. Over the years Josh has developed knowledge and skills that enable him to access almost any computer and database in his company with or without authorization. The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or nonconfidential data. Josh has been working on multiple projects recently, some with deadlines in one or two weeks. Josh is under tremendous press to meet the deadlines of his boss. Josh is also financially stressed and he is behind in some payments for his bills and credit cards. In all of the following scenarios, imagine that you are Josh …	To set up the scenario background

3.1 Practice Scenarios

Practice scenarios are designed to get the test participant to be familiar with the test process and the keyboard controls used for the testing. It is also time used to train participants to remain steady during the remainder of the test.

Practice scenarios and stimuli

Scenario 1	Josh receives an e-mail from Microsoft that there is a local training seminar on Wednesday afternoon about managing security.
Prompt	Should Josh go to the seminar?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 2	Josh was planning to take an advanced computer security course in a local university starting next week.
Prompt	Should Josh take the course?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 3	Josh had planned a family vacation to Europe in the summer, but he just heard that the company is going to reorganize and there will be layoffs.
Prompt	Should Josh go on vacation?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 4	Josh received an e-mail from his manager that the company is going to honor him and others for their loyalty in a ceremony.
Prompt	Should Josh attend the ceremony?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 5	Josh is about to leave work for a Friday-night game when he notices the company's Web server is having unusual activity.
Prompt	Should Josh stay and figure out the problem?
	No (1) Likely no (2) Likely yes (3) Yes (4)

3.2 Control Scenarios and Stimuli

Control scenarios are those that involve routine decisions an individual faces in everyday life and they do not involve information security situations. These decisions are usually nonconsequential.

Control scenarios and stimuli

Scenario 1	Josh received an e-mail from a local university about a one-day IT security seminar on the upcoming Friday from his college professor.
Prompt	Should Josh attend?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 2	Josh's best friend Eric, who works for a competitor, called to ask if he is interested in going to an NBA basketball game on Wednesday evening.
Prompt	Should Josh go to the game with Eric?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 3	Josh's girlfriend Jenny, who works for a consulting firm, asks Josh if he can take a day off this week to help her on a project she needs to complete that week for her firm.
Prompt	Should Josh take the day off to help Jenny?
	No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 4	Josh's buddy Mike, who works for an investment firm, wants to play golf on Saturday with Josh.

(continues)

Control scenarios and stimuli

Prompt	Should Josh play golf on Saturday with Mike? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 5	Josh's boss Christine asks Josh to spend a day helping her on a project she needs to complete by Friday.
Prompt	Should Josh help Christine on her project? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 6	Josh's brother-in-law Kevin, who is a salesperson for a local firm, asks Josh if he could join him and a few other friends for weekend hiking into the mountains for two days.
Prompt	Should Josh join the group and hike for two days? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 7	Josh's mentor Mary asks Josh if he could cover for her for one day on Friday so she can attend a family reunion in another city in the weekend.
Prompt	Should Josh cover for Mary for one day? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 8	Josh is not sure about how much he should be asking for a salary raise or even if he should be asking at all since the company has not been doing well recently.
Prompt	Should Josh ask for an increase? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 9	Josh belongs to a citizens' group that advocates hiring local workers. The group asks Josh to distribute brochures in his company.
Prompt	Should Josh distribute these brochures in his company? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 10	Josh met a fellow IT professional, Frank, at an industry conference in Las Vegas. Frank asks Josh if he could share some best practices in managing IT services with his company.
Prompt	Should Josh share these practices with Frank? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 11	Josh's company is receiving bids for a multimillion-dollar manufacturing contract from suppliers. An old friend who works for a supplier called to ask Josh to have dinner with him on Friday night.
Prompt	Should Josh go to dinner with this friend? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 12	Josh's buddy Mike, who works in the sales department, asked Josh to create a nonstandard sales report for him. This may take hours and is not part of Josh's job.
Prompt	Should Josh help Mike create this report? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 13	Josh's friend Jane, who works as a payroll specialist, has entered incorrect hours for a few hourly employees. She asks Josh to correct these errors without alerting her boss.
Prompt	Should Josh correct the errors for Jane? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 14	Josh has to work overtime in the next few days to complete a project by this coming Friday. However, a long-scheduled dinner with his brother's family is tonight.

(continues)

Control scenarios and stimuli	
Prompt	Should Josh go to the dinner? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 15	Josh has invested all of his savings in stocks and he is nervous about it. He wants to monitor stock prices and do research on stocks using the Internet at work.
Prompt	Should Josh do stock research while at work? No (1) Likely no (2) Likely yes (3) Yes (4)

3.3 Minor Violation Scenarios and Stimuli

Easy scenarios are those that involve routine decisions an individual might face in a typical work environment that are related to information security situations. These decisions usually have nonsignificant consequences to the individual or the organization.

Minor violations scenarios and stimuli	
Scenario 1	Josh received an e-mail from his college professor who asked Josh to talk about the details of IT security management, which is considered confidential, in a seminar.
Prompt	Should Josh honor his professor's request? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 2	Josh's best friend Eric, who works for a competitor, wanted to know whether a new product under development has certain features.
Prompt	Should Josh access the secure server and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 3	Josh's girlfriend Jenny, who works for a consulting firm, wanted to know whether one of her clients is involved in the new product development with his firm.
Prompt	Should Josh access the secure server and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 4	Josh's buddy Mike, who works for an investment firm, wanted to know how close a new product under development is to commercial production.
Prompt	Should Josh access the secure server and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 5	Josh's boss Christine wanted to know about the executive compensation information of the company, which is confidential.
Prompt	Should Josh access the secure server and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 6	Josh's brother-in-law Kevin, who is a salesperson for a local firm, wanted to know if a particular type of material is used in the new product under development.

(continues)

Minor violations scenarios and stimuli	
Prompt	Should Josh access the secure server and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 7	Josh's mentor Mary is worried about her job security and wanted to know if her position is among those that are being considered for elimination.
Prompt	Should Josh access the secure server and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 8	Josh is not sure how much he should be asking for a salary raise or even if he should be asking at all given the financial situation of the company.
Prompt	Should Josh access the secure server and find more information? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 9	Josh belongs to a citizens' group that advocates hiring local workers. The group wanted to confirm whether Josh's company is outsourcing jobs to offshore suppliers.
Prompt	Should Josh access the secure server and find it out? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 10	Josh met Frank at an industry conference in Las Vegas. Frank asks Josh if he could give him the IP address of a highly protected computer server for testing.
Prompt	Should Josh finds out the IP address for Frank? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 11	At a dinner with friends Josh was introduced to a stranger who asked if Josh knows the price of a component for which Josh's company is requesting bids from suppliers.
Prompt	Should Josh get the price on a secure server for this stranger? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 12	Josh's buddy Mike, who works in the sales department of the same company, wanted to know if another account manager in the company is about to close a major deal.
Prompt	Should Josh access the secure server and get the information? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 13	Josh's friend, Jane, works in the HR department as a payroll specialist. Jane asked Josh to change the payroll data file to erase the unpaid vacation hours she had taken.
Prompt	Should Josh make the changes on the server for Jane? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 14	The only way for Josh to meet the deadline this Friday is to bring some files home to work on his computer in the evenings, which is explicitly prohibited by the company.
Prompt	Should Josh bring the files home and work on his computer? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 15	Josh has invested a significant portion of his money in his company stock. The new product under development is going to have a significant impact on the stock price.
Prompt	Should Josh find internal documents about the new product? No (1) Likely no (2) Likely yes (3) Yes (4)

3.4 Major Violation Scenarios and Stimuli

Hard scenarios are those that involve nonroutine decisions an individual might face in a typical work environment that are related to information security situations. These decisions usually have significant consequences to the individual or the organization.

Major violation scenarios and stimuli

Scenario 1	Jeff is an IT consultant Josh met at a seminar. Jeff wants a copy of the detailed computer network map of the company, and offers Josh a chance of making a substantial amount of money on a consulting project.
Prompt	Should Josh provide the map? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 2	Josh's buddy Eric, who works for a competitor, wanted to get a critical design in the new product under development, and promises to pay a substantial amount of money.
Prompt	Should Josh access the secure server and find the data for Eric? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 3	Josh's girlfriend Jenny, who works for a consulting firm, wanted to have some information about suppliers. Jenny could earn a substantial amount of commission.
Prompt	Should Josh access the secure server and find the data for Jenny? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 4	Josh's friend Mike, who works for an investment firm, wanted know the quarterly earnings data before public release, and promised to share any profit from this data.
Prompt	Should Josh access the secure server and get the data for Mike? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 5	Josh's boss Christine wanted to know the compensation information of the top executives in the company. Josh could earn substantial favors from Christine.
Prompt	Should Josh access the secure server and get the data for Christine? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 6	Josh's brother-in-law Kevin, who is a salesperson for a local firm, wanted to get contract information of suppliers, and promised to share a substantial amount of commission.
Prompt	Should Josh get the information for Kevin? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 7	Josh's mentor Mary was laid off due to downsizing. Josh is very upset about this and considering doing something to take revenge.
Prompt	Should Josh delete crucial computer files to vent his anger? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 8	Josh has been upset about not receiving an anticipated salary increase in the last annual evaluation. He knows some underground websites offering to pay for credit card data.

(continues)

Major violation scenarios and stimuli	
Prompt	Should Josh sell customer credit card information? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 9	Josh belongs to a citizens' group that advocates hiring local workers. The group wants Josh to provide some confidential evidence to support a lawsuit. Josh would share any settlement money if the group wins.
Prompt	Should Josh provide the confidential data to the group? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 10	Josh met Frank at an industry conference in Las Vegas. Frank asks Josh if he could give him the IP address of a highly protected computer server for testing, and promises to help Josh find consulting work.
Prompt	Should Josh give Frank the information? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 11	At a dinner with friends, Josh was introduced to a stranger who asked if Josh knows the bidding price of a component from suppliers, and promised to share commission.
Prompt	Should Josh get the price for this stranger? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 12	Josh's buddy Mike, who works in the sales department, wanted to know the prices of competitors for similar products to those he is selling, and promised to share commission.
Prompt	Should Josh access competitors' computers and find the data? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 13	Josh's friend Julie, who is an HR manager, asks Josh to find payroll information of peer companies for her benchmark study, and promises Josh to help in the future.
Prompt	Should Josh access the payroll data on peer companies' servers? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 14	Josh must complete a project by this Friday and one way to speed up the progress is to copy source code from other companies that he knows have done similar projects.
Prompt	Should Josh hack into a competitor's computer and copy the code? No (1) Likely no (2) Likely yes (3) Yes (4)
Scenario 15	Josh's company is about to release quarterly earnings. If he can act early before the information is public, he could make a substantial profit on the stock market.
Prompt	Should Josh find out the earnings data and act accordingly? No (1) Likely no (2) Likely yes (3) Yes (4)