2014 47th Hawaii International Conference on System Science

Why Individuals Commit Information Security Violations: Neural Correlates of Decision Processes and Self-Control

Qing Hu
Iowa State University
qinghu@iastate.edu

Robert West
Iowa State University
rwest@iastate.edu

Laura Smarandescu
Iowa State University
smarand@iastate.edu

Zachary Yaple
Iowa State University
zyaple@iastate.edu

Abstract

Self-control has been identified as a major factor influencing individual behavior in social studies, economics, criminology, and information security literatures. Recent neuroscience studies show that lack of self-control can be attributed to lesions in the right prefrontal region of the brain, suggesting a strong linkage between self-control and neural processes. In this study, we tested neural correlates between self-control and decision making in the context of information security using electroencephalography (EEG) and event related potentials (ERPs). Our results show that while both left and right hemispheres of the brain are involved in decision making, the subjects with low self-control evoked lower level of neural activities in the right hemisphere and made riskier decisions than the subjects with high self-control. This study validates a new paradigm for using EEG/ERP to study information security related phenomena, and opens a new path for studying decision making neural correlates using scenario based approach.

1. Introduction

In the information security defensive chain around the digital assets of an organization, human agents have often been identified as the weakest link [6, 20]. This is because the effectiveness of other elements in the security defense, such as security technology, organizational policies and procedures, as well as government regulations and laws, are largely dependent on the effort of the human agents, especially those who work with the digital assets on a daily basis within organizations.

In fact, human agents inside an organization could potentially be more dangerous than those outside the organization due to their intimate knowledge about the organizational information systems and the permissions they receive either properly or improperly for their routine work activities. In a recent survey of IT managers of global companies, 60% of the respondents said that employee misconducts involving information systems is a top concern about information security, second only to major computer viruses [12]. According to Symantec and Ponemon [32], 59% of ex-employees admit that they steal confidential company data, such as customer contact lists, from their former employers.

Can we predict which employee would be more likely rule-abiding when entrusted with sensitive and valuable digital assets in organizations? Do we know why some employees are better than others in resisting temptations of short-term gain in order to achieve more significant long-term benefits? There is a plethora of management, economic, and psychological theories about human motivation and behavior in the context of information security (e.g., [6, 9, 18, 20, 31]). However, most of them are based on interviews and surveys that rely on self-reporting, which has been plagued with issues like common method bias or social desirability [23, 28]. Recent advances in cognitive neuroscience, however, have provided a unique opportunity to study human behavior without much of the biases common in traditional behavioral research in management literature.

We believe that neuroscience research techniques and methodologies can make a significant contribution to studies aimed at understanding 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 observe and collect data directly from the human brain while research subjects are contemplating with various decision options, and establish neural correlates between decision outcomes and brain processes. Perhaps more interesting to social scientists, the neurocognitive approach based on brain imaging technologies can significantly minimize the effect of social desirability bias in subject responses because few brain processes can be consciously manipulated by the subjects after stimuli onset.

Thus, we set out to conduct an EEG based event related potential (ERP, a measure of the brain's electrophysiological response to a specific sensory, cognitive, or motor stimulus) study of the neural basis of human decision making related to rule abiding/breaking behavior in the context of information security. In doing so, we hope to advance information security research, and develop a more sophisticated research paradigm for understanding of human decision making in general.

2. Theory and Hypotheses Development

The concept of self-control has attracted significant interests from psychologists [11, 21]; criminologists [1, 13, 14, 36], neuroscientists [15, 19, 24], and more recently information security scholars [18]. Muraven

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.400

and Baumeister [26] defined self-control as the exertion of control by one over the self; therefore, self-control occurs when the person attempts to change the way he or she would otherwise think or behave under given stimuli and circumstances. They further argued that self-control behaviors are designed to maximize the long-term best interests of the individual, and people exert self-control when they follow rules or inhibit immediate desires to delay gratification.

In criminological research, one of the preeminent theories is self-control theory [13]. This general theory of crime is developed to explain a wide range of criminal activities in society. Gottfredson and Hirschi [13] argued that all human beings have the same potential of committing crimes given the right circumstances; however, not everyone become criminals because of individual differences in self-control – ability to refrain from committing deviant or criminal acts under given circumstances. This ability is said to be established early in life and remains relatively stable throughout an individual's lifespan. Criminal behavior is likely to occur when individuals with low self-control are presented with opportunities for committing crimes. Gottfredson and Hirschi [13] 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 for criminological inquiries [10], and has accumulated strong empirical support [27]. Low self-control has been found to have direct and indirect influence on criminal behavioral intentions. For example, in a study of shoplifting behavior of college students, Piquero and Tibbetts [27] found that low self-control not only has a direct effect on intentions to shoplift; it also indirectly affects intentions to shoplift through situational variables (pleasure and shame). Vazsonyi et al. [34] found low self-control is directly linked to a number of deviant behaviors in both genders and across different age groups, and the effects appear to be nation and culture invariant in a large scale study of youth (N=8,417) in four nations. Wright et al. [37] also provided strong evidence for the critical role of low self-control in adult criminal behavior and intentions in a study based on longitudinal data of individuals from age 5 to age 26.

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" [13, p. 91]. This provides the foundation for IS scholars to use this theory in understanding information security offenses committed by individuals. Higgins et al. [17] was among the earliest studies that used low self-control in studying individual behavior in information security context. The authors found that low self-control, along with certainty of deterrence, was significantly associated with software piracy behavior among college students. Similarly, Zhang et al. [38] tested the impact of low self-control and deterrence on digital piracy (illegal copying of digital products such as software, documents, video, and audio) behavior of college students. The authors found that only the risk-taking dimension of low self-control and the certainty dimension of the deterrence have a significant impact on the focal behavior.

The extant literature suggests that self-control plays a significant role in human behavior, from economic decisions and social conducts to substance abuse and criminal activities. However, one critical question that still remains debatable among 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 impact of self-control on behavior and decision and those that support an indirect impact of self-control on behavior and decision. The direct impact 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 (e.g., [10, 13, 14, 34]). The indirect impact camp, which is more dominant in criminological literature, argues that rational choice is the fundamental process of human decision and behavior, and therefore, the impact of self-control on human behavior and decision is through altering of the evaluation parameters in rational calculus, such as increasing the perceived benefits and decreasing perceived costs for intended actions, or interacting with other decision parameters, such as moral values and social learning when criminal or deviant opportunities are presented (e.g., [18, 27, 29, 30, 36]).

While the two schools of literature disagree on how exactly self-control contributes to deviant behavior, the literature is fairly consistent that low self-control, as measured by Grasmick et al. [14], leads to individuals to think more about short-term reward and less about long-term consequence, thus more likely to take risk for immediate gratification. In situations where violation of established information security policies may provide immediate reward, we argue that:

> ***Proposition 1***: *Individuals with low self-control have a tendency to choose riskier actions for near-term reward in contrast to those with high self-control when contemplating decisions that have potentially long-term negative consequences in the context of information security policy violations.*

Given the reliance on survey research methodology and the complications of associated common method bias, there appears little chance that these two schools can consolidate their findings and reach some sort of consensus. However, recent discoveries in neuroscience and neuroeconomics studies have offered some hope and generated significant insights on how self-control influences human behavior and decision making, with direct observations of human brain activities when relevant decisions are contemplated by research subjects under various real or simulated decision making conditions. Self-control, sometimes referred to as willpower or impulse control in neuroscience literature [3, 4], has been directly linked to the brain functions in the ventral medial prefrontal cortex (VMPFC) [3, 15], especially the right ventral medial prefrontal cortex (rVMPFC) [4, 22, 33], using functional magnetic resonance imaging (fMRI) technology.

The most interesting finding of these neuroscience studies to our research is that in patients who had lesions in their rVMPFC or right prefrontal region (rPFC), there are significant deficits in social conduct, decision-making, risk management, and emotional processing, in comparison to those patients who had only the left side lesions, or to the control groups [7, 33]. Knoch and Fehr [22] provided even more direct evidence of the role of rPFC in self-control by temporarily disrupting the brain function in this region. In their study, the researchers used a low-frequency repetitive transcranial magnetic simulation (rTMS) to disrupt left or right dorsolateral prefrontal cortex (DLPFC) function transiently before applying a gambling task to measure risk taking behavior of healthy adults. They found that individuals with right DLPFC disruption displayed a significantly stronger preference for choosing the larger potential reward at the risk of even greater penalty, while those with left DLPFC disruptions did not and performed similarly as those with sham treatment. This is further corroborated by Boes et al. [4] using healthy school age boys. They found that the rVMPFC is a significant predictor of impulse control ratings provided by parents and school teachers of these boys; and fMRI data revealed that the rVMPFC volume is significantly lower in the subgroup of 20 impulsive subjects compared to the subgroup of 20 non-impulsive ones.

These studies provide strong evidence for us to argue that the psychological construct self-control is rooted in the physical neural structures of the human brain, especially in the rVMPFC region, at least in the right hemisphere. A damaged or under-developed rPFC or rVMPFC is likely to cause an individual to have diminished ability for self-control, as indicated by impulsive behavior, preference to risky choices, and disregard to long-term negative consequences. With ERP methodology, while we cannot pinpoint the exact locations where relevant brain processes are evokved, we can, however, detect the evocation in the right and left hemisphere with millisecond accuracy. This discussion leads to our second proposition:

> ***Proposition 2****: Individuals with low self-control tend to evoke less brain activities in the right hemisphere in contrast to those with high self-control when contemplating decisions that have potentially long-term negative consequences in the context of information security policy violations.*

To investigate these propositions, we designed and carried out two neuroscience studies using ERPs based on EEG signals evoked during simulated decision making in the context of information security policy violations in organizational settings. Although the majority of the reference studies on self-control and behavior in neuroscience literature use brain imaging technologies such as fMRI, we chose EEG/ERP for two primary reasons. The first and foremost is the high temporal resolution of EEG/ERP, accurate to millisecond level, in contrast to fMRI which usually takes seconds after stimulus onset to produce usable data. Given the difficulty in detecting true responses of individuals when presented with an information security scenario, it is critical to measure what happens in the brain in milliseconds, instead of seconds, after stimulus onset, to minimize social desirability bias contamination. The second reason is the low cost of EEG/ERP experiment relevant to fMRI, which affords researchers to study larger samples in comparison to studies using fMRI.

3. Methodology

3.1 Participants

Participants for this study were 42 English speaking subjects (40 males, 2 females, age 19 to 24, all right handed), recruited from a subject pool about 350 undergraduates attending a large Midwest public university. Students signed up for the research pool voluntarily, and if they were selected for participation in the studies, they received a small course credit and potentially monetary reward. We created two subject pools for the two studies in this research. Study 1 aimed at developing and validating the test paradigm for using EEG/ERP techniques in information security research. This study involved 20 (18 males and 2 females) student subjects randomly selected from the general subject pool. Study 2 was for investigating the research propositions once the test paradigm was validated. This study involved 22 (all males) student subjects also selected from the general subject pool but based on their self-control scores using a survey instrument adapted from Grasmick et al. [14]. Only those subjects who had a score in the top 25% (low self-control) and bottom 25% (high self-control) were invited to participate. There is no overlap of subjects between the

two studies. The reason for using only the subjects 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, were given the Informed Consent form prior to the inclusion of the study.

To motivate truthful responses from the subjects, we designed a paradigm that involved some degree of deception, with the approval of our Institutional Review Board. All subjects in the general pool were invited to take a 68-item survey that include demographic data, self-control measurement, and moral judgment and decisions related to three information security policy violation scenarios. Then, for all subjects selected to participate in the research, before the data collection started, each subject was informed that the computer software has developed a psychological profile based his/her responses to the survey, and s/he would be paid anywhere from $15 to $25 based on how the responses during the study matches the established profile; and the best strategy to make most money is to answer the questions as truthful as possible. In fact, there was no psychological profile established, and the computer generated random amount between $23 and $25 to pay for each subject at the end. The very narrow payout range was designed to minimize the psychological effect on a subject had s/he received a low payment amount. All subjects were debriefed about the protocol after the study was completed.

3.2 Stimuli

In order to evoke relevant brain electrophysiological processes that emit measurable EEG signals from human subjects making information security related decisions, we faced two significant challenges. The first challenge was how to make our research subjects experience information security decision making in a controlled laboratory setting. The second challenge was how to design the experiments so that the relevant brain processes are evoked and strong enough EEG signals can be detected and recorded for later processing using existing lab equipment and software.

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 subjects in criminal or deviant situations (e.g., [9, 16, 27, 30, 31]). Due to the secrecy involved in criminal or deviant behavior, it is natural that individuals are unwilling or uncomfortable to report 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 subjects.

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, easy, and hard, a total 45 stimuli based on information security scenarios. Table 1 provides a definition for each category with a sample scenario for illustration.

Table 1: Scenarios and Examples

Definition	Sample Scenario
Control scenarios involve routine decisions an individual makes in everyday life that do not involve information security and are usually non-consequential.	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. Should Josh take a day off to help Jenny?
Easy 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. Should Josh access the secure server and find out for Jenny?
Hard 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 substantial amount of commission. Should Josh access the secure server and find the data for Jenny?

We addressed the second challenge with two treatments included in the experiment design. The first treatment was to motivate the subjects to be truthful in their responses, which was accomplished by a 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, easy, and hard) with 15 different variations each using a pseudorandom order (the order of the stimuli presentation were randomized but consistent across all subjects), which is common technique in studies involving EEG/ERP. All of the stimuli were programed into the E-PRIME software (PST, Inc., Pittsburgh, PA) using white on black background to reduce the influence of luminance on the ERP waveforms.

To simulate real world situations as closely as possible and evoke relevant neural activities, before the test stimuli were presented, the subject was primed with a scenario as follows. Imagine that s/he was Josh, an IT professional working in the IT department of a large global manufacturing company. The company supplies sophisticated electronic control instruments for civilian and military uses. 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 non-confidential data. Josh is working on multiple projects recently, some with deadlines in one or two weeks, so Josh is under tremendous pressure to meet the deadlines. Josh was also financially stressed and he was behind some payments for various bills and credit cards.

3.3 Procedure

We followed the common practice in EEG/ERP studies when designing our experiment procedure. Once a subject has been hooked up to the data collection equipment, the priming screen is presented first. When the subject presses the "Next" button, five practice scenarios are 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 test scenarios, but involving no information security related decision making. After the 5 practice trials, the test scenarios are presented. Once a test scenario is presented on screen, the subject presses any button on the key pad to proceed to the decision screen. A 500ms delay is introduced to fixate the eyes on the center of the screen before the decision button screen is presented. There is no time limit on how long the decision screen is displayed. As soon as the subject presses one of the decision buttons, the next scenario is presented. This process repeats 45 times for each subject and then the test is complete. The computer displays a reward amount on the screen and the subject is paid after completing a post experiment survey. Figure 1 demonstrates the rapid serial visual presentation (RSVP) procedure for both Study 1 and Study 2.

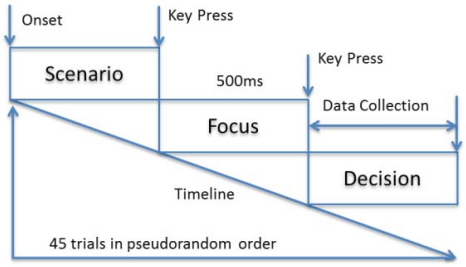

Figure 1: The RSVP Procedure for Data Collection

When a subject enters the lab at the assigned time slot, the subject is briefed about the study, and the Informed Consent form approved by the IRB is given to the subject to read and sign. The subject is then directed to the sound damped and electrically shielded data collection booth and seated in a comfortable reclining armchair. The subject is placed approximately 15-20 inches from the computer monitor that displays the stimuli and decision choices. The EEG data collection cap is then mounted on the head of the subject by the research assistants. Raw EEG data are recorded using Sensorium software package. No breaks are given throughout the experiment.

3.4 Electrophysiological Recordings

For both Study 1 and Study 2, the electrode impedance was lower than 20 kΩ for all subjects. During recording, a nose reference was used and the data were re-referencing to a common average for analysis. Horizontal electrodes were placed 1 cm lateral of the outer canthus of each eye to monitor horizontal ocular movements (EOG). Vertical EOG was recorded by placing two electrodes 1cm above each eye. The ground electrode was located 10 mm anterior to the Fz electrode. Figure 2 shows the relative locations of the electrodes on the EEG data collection cap.

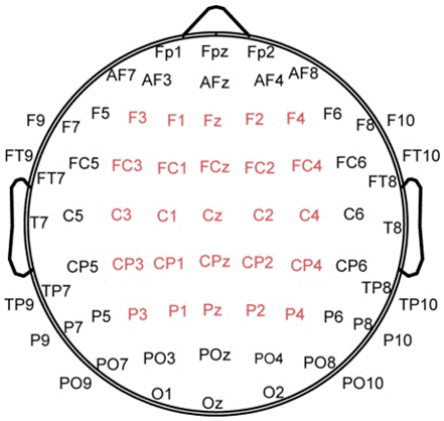

Figure 2: Relative Locations of Electrodes

The data were processed using the EMSE software. The EEG signals were sampled at 2048 Hz from 65 electrodes. A bandpass digital filter between 0.1 and 20 Hz was applied offline. An EEG epoch length of 2200ms was used with a 200ms pre-stimulus baseline correction and 2000ms following stimulus onset. Epochs were rejected from averaging if amplitude exceeded +/- 100μV, and eye blinks were corrected using the ocular artifact correction filter in EMSE. Artifact-free segments were averaged to obtain the ERPs per subject. No participants had less than 80 percent accepted trials in any condition.

4. Results and Analyses

The ERP grand average waveforms were averaged separately for each experimental condition across subjects. For ERP statistical analysis, repeated measures ANOVA and Independent Samples t-Test were used to test differences in mean ERP activation in the time window 500–1000ms post stimulus for Study 1 and 300–600ms post stimulus for Study 2. The wider ERP epoch window was used in Study 1 because of its exploratory nature. Once the paradigm was established,

a narrower epoch was used in Study 2 for data analysis that focuses on interesting ERP waveforms at relevant electrodes.

To the best of our knowledge, no test paradigms have been specifically designed and validated for research in the context of information security or even criminology. As a laboratory based scientific research methodology, EEG/ERP studies rely on validated paradigms for producing reliable and replicable results. Therefore, the current research had two primary objectives that were accomplished in two studies. In Study 1, we developed and validated a new paradigm modeled after the existing work related to criminology and information security research and appropriate for use with EEG/ERP techniques. In Study 2, we then used this validated paradigm to examine the influence of individual differences in self-control on neural activities related to decision processes in the context of information security.

4.1 Study 1 – Validation of Paradigm

The primary objectives of Study 1 is to design and validate a paradigm to ensure that 1) measureable ERP data are generated from test subjects 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. 20 subjects (18 males and 2 female) participated in the study, and EEG data were recorded using the procedures and parameters described in the previous section. Figure 3 shows the grand averaged ERP waveforms of the 20 subjects at six frontal and frontal-temporal electrodes located in the left and right hemisphere of the scalp.

The ERPs clearly demonstrate the effect of difficulty levels of the scenarios related information security policy violations on the left and right frontal region of the brain. The tall bar reflects stimulus onset of the decision screen (time 0) and the short bars reflect 200ms increments. Note the differences in amplitude among the three conditions that emerged around 300ms after onset of the decision cue on the left hemisphere (F7, FT7, and FT9) and the right hemisphere (F8, FT8, and FT10). These differences suggest that the three categories of stimuli we created based on scenarios of various information security policy violations in organizational context indeed evoke distinguishable ERP waveforms, providing strong evidence of validity of the paradigm designed for this study.

Figure 3 also reveals the first important finding of the study: two new ERP components that have not been widely reported or studies in the neuroscience literature: a left frontal negativity (LFN) and a right frontal positivity (RFP). The LFN component is shown in ERP waveforms of the left hemisphere (F7, FT7, and FT9) electrodes. It starts at about 300ms after onset of the decision cue, and lasted until about 1500ms after onset of the decision cue. In contrast, the RFP component is shown in ERP waveforms of the right hemisphere (F8, FT8, and FT10) electrodes. It starts also at about 300ms after onset of the decision cue, and lasted until about 1500ms after onset of the decision cue.

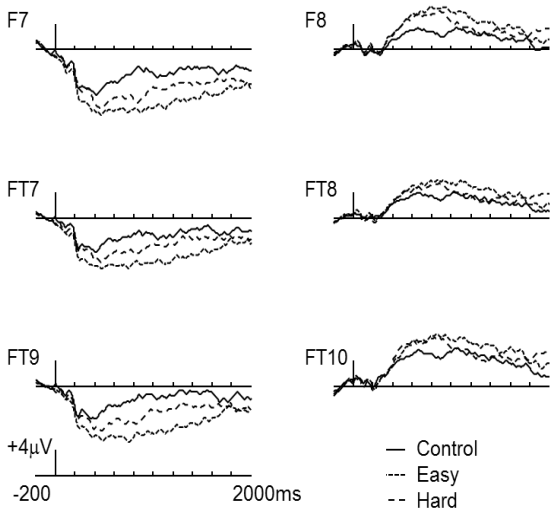

Figure 3: Grand-Averaged ERPs at Left and Right Hemisphere Electrodes

To further confirm that the differences among the grand-averaged ERPs components (LFN and RFP) generated from the three categories of stimuli are statistically significant, we also run Independent Sample t-test using the ERP amplitude data from 500ms to 1000ms after onset of the decision cue. The results are shown in Table 2 and Figure 4.

Tests with ERP data at other electrodes in the frontal and frontal-temporal regions produced similar results but not presented here to reduce redundancy. These results suggest that our test paradigm has accomplished the stated design objectives. It provided the scientific foundation for Study 2 to investigate the research propositions using this paradigm.

Table 2: Comparison of Means of ERP Activation between Stimuli Conditions

Electrode	Stimuli Category	ERP (500-1000ms)		Group Mean Comparison	
		Mean	Std.	Pairs	t-Stats (p)
Average of Left Hemisphere (F7, FT7, FT9)	Control	-3.26	1.18	C-E	**4.665** (.000***)
	Easy	-8.40	1.48	E-H	**3.105** (.006***)
	Hard	-6.26	1.48	C-H	**-1.766** (.090*)
Average of Right Hemisphere (F8, FT8, FT10)	Control	3.67	1.40	C-E	**-2.820** (.011**)
	Easy	6.15	1.53	E-H	**-3.097** (.006***)
	Hard	5.62	1.50	C-H	.554 (.586)

*p<0.1, **p<0.05, ***p<0.01

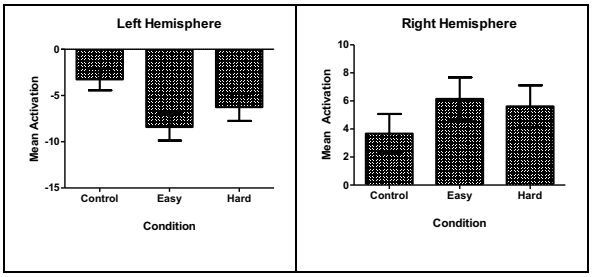

Figure 4: Differences in ERP Activation between Stimuli Conditions

4.2 Study 2 – Testing of Hypotheses

The primary objective of Study 2 is to investigate the propositions of this study: that the low self-control individuals tend to make riskier decisions that have near-term reward but long-term negative consequences, and they evoke lower level of ERPs in the right hemisphere in contrast to the high self-control individuals when making information security policy violation related decisions.

As described in the previous section, 22 subjects were recruited for this study, including 11 low self-control and 11 high self-control individuals based on their scores on the Grasmick et al. [14] scale. The paradigm validated in Study 1 was used for carrying out the experiment and data collection. As described in 3.3, we recorded a subject's decision as well as EEG data during a test session. The decision data were analogues to survey responses. For each information security related stimulus, a subject chose a value from 1 to 4 by pressing the corresponding button. Table 3 shows the mean comparison of decision choices between the high and low self-control subjects with three stimulus categories.

Table 3: Test of Sample Means of Decision Choices between Groups

Stimuli Category	Self-Control	Decision Choice		Group Means Comparison	
		Mean	Std. Div.	F-stat (p-val.)	t-Stats (p-val.)
Control	H	2.653	.384	3.382	-.229
	L	2.385	.237	(.082)	(.821)
Easy	H	1.273	.290	.132	**-2.422**
	L	1.576	.297	(.721)	(.025**)
Hard	H	1.140	.195	2.246	**-2.087**
	L	1.356	.272	(.150)	(.051*)

*p<0.1, **p<0.05, ***p<0.01

Two interesting results can be seen from this table. First, there is no statistical difference between the low and high self-control subjects with the control stimuli, and the average choice is between 2 and 3, right in the middle of the decision range. This suggests that the control stimuli are valid and generated expected responses in both groups. Second, the decision choices between the low and the high self-control subjects in Easy and Hard conditions are indeed statistically different, and as we predicted, the low self-control subjects made riskier choices than the high self-control subjects, albeit slightly, but still statistically significant in both Easy and Hard stimulus conditions. Thus, Proposition 1 is supported by our data.

The EEG data collected were used to compute ERPs of the subjects when they were contemplating the decision choices. The average decision time for all subjects was about 2000-2500ms after stimuli onset (Easy: mean=2383ms, se=209ms; Hard: mean=2041ms, se=145ms; Control: mean=2457ms, se=139ms). Figure 4 shows the grand-averaged ERP waveforms at the left hemisphere (FT, FT7, and FT9) and the right hemisphere (F8, FT8, and FT10) electrodes.

There are several interesting observations from the ERP waveforms presented in Figure 5. First of all, the ERP components discovered in Study 1, LFN and RFP, are reproduced in Study 2, providing further evidence of the reliability of the paradigm. Second, while the ERP waveforms of the electrodes in the left hemisphere are similar between low and high self-control individuals, the RFP component is quite different between the two groups at the right hemisphere. As we have expected, individuals with low self-control appear to evoke reduced amplitude of ERPs in contrast to individuals with high self-controls.

To further verify the findings, we conducted multiple repeated measures ANOVA analyses. As in Study 1, we compared within group pairwise means of the ERP amplitudes generated by the three categories of stimuli. In addition, we also compared between group pairwise means of the ERP amplitudes. These results are shown in Figure 6 and Table 4.

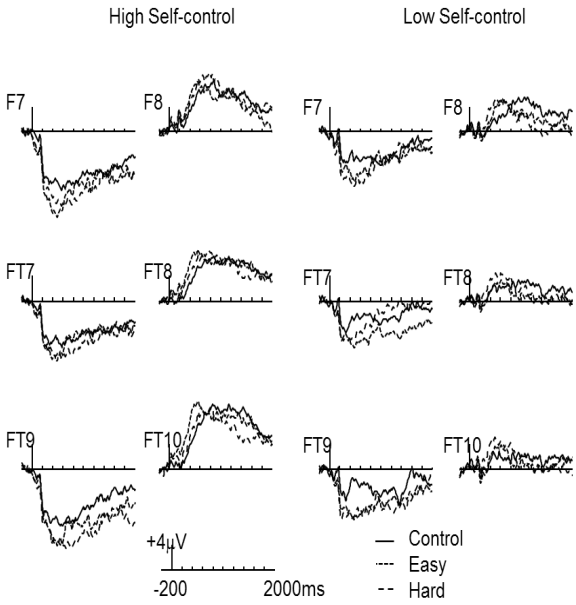

Figure 5: Grand-Averaged ERPs at Electrodes on Left and Right Hemisphere between Groups

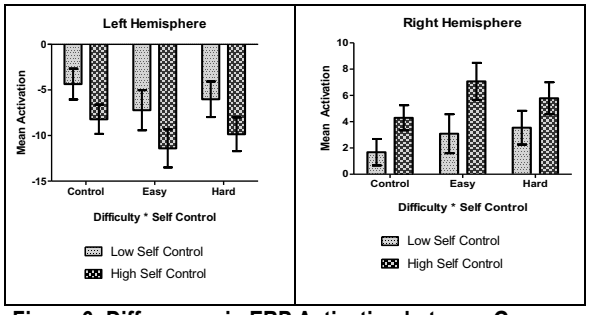

Figure 6: Differences in ERP Activation between Groups

Table 4: Comparison of Means of ERP Activation between Stimuli and Groups

Electrode	Stimuli Category	Group by Self-Control	ERP (300-600ms)		Group Mean Comparison
			Mean	Std.	t-Stat (p)
		High	6.46	3.53	
Average Electrodes Left	Control	Low	-4.35	4.78	1.657
		High	-8.22	5.33	(.12)
	Easy	Low	-7.24	5.30	1.376
		High	-11.40	7.57	(.19)
	Hard	Low	-6.02	5.91	1.427
		High	-9.86	5.81	(.17)
Average Electrodes Right	Control	Low	1.68	3.39	**-1.885**
		High	4.30	2.65	(.08*)
	Easy	Low	3.09	4.87	**-1.949**
		High	7.07	4.04	(.07*)
	Hard	Low	3.55	4.25	-1.266
		High	5.79	3.47	(.23)

*p<0.1, **p<0.05, ***p<0.01

The t-tests of Independent Samples confirm that the differences in mean amplitudes of ERP component LFN (300-600ms) at electrodes on the left hemisphere between low and high self-control subjects are not statistically significant (p>0.1); while the differences in mean amplitudes of ERP component RFP (300-600ms) at electrodes on the right hemisphere between low and high self-control subjects are significantly different (p <0.1) with Easy stimuli, but not significant with Hard stimuli. Note that the sample size is small (N=11) and the variances are large for both groups. With larger samples, we anticipate more significant differences may be detected. This result provides moderate support for our Proposition 2.

5. Discussion

This study and the main findings presented above have some interesting theoretical and practical implications for information security and human decision making in general. Our findings, along with other neuroscience studies (e.g., [3, 4, 15, 22, 33]), show that self-control is directly linked to neural processes in the brain of an individual, especially in the right hemisphere of the brain. This is important because it supports Gottfredson and Hirschi [13]'s assertion that self-control is a characteristic of an individual, formed early in life, and remains relative stable throughout the lifespan. Therefore, an individual's self-control characteristic cannot be easily altered by environmental dynamics later in life such as training or learning in organizations.

The second contribution of this study is the development and validation of an EEG/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 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 start using it, a solid foundation has been established for future research using this type of methodologies.

The third contribution of this study is the identification of the new ERP components LNR and RPR in the frontal and frontal-temporal region, which appear to be unique to this new paradigm we have established. We found no similar components in the prior EEG/ERP studies that involve human decision making (e.g., [2, 5, 8, 25, 24]). The identification of these two new ERP components enables future research to have reference points and continue to accumulate knowledge related to human decision making in the context of information security.

Finally, our findings may also help reconcile the on-going debate whether humans are rational or irrational in decision making literature. The evidence suggests that high self-control individuals, who appear to be more rational, recruit both left and right hemisphere of their brain, in contrast to the low self-control individuals, who appear to be less rational or irrational to some sense, recruit mostly the left hemisphere of their brains, when making difficult decisions. Thus, humans are neither completely rational nor completely irrational by default. It all depends on how each individual developed their characteristics during the formative years. As a result, some individuals appear more rational, and others appear more irrational, in making decisions.

Our findings have at least two important practical implications. First, we have shown that the instrument developed by Grasmick et al. [14] is a reliable and valid measure of individual self-control. In the literature there are multiple versions of self-control scales developed by psychologist and criminologists. Our results showed that the individuals identified as having high and low self-control using the Grasmack [14] scale have consistent ERP and behavioral characteristics as those identified by neuroscientists with more sophisticated means.

Perhaps the most important practical implication of our findings is that self-control screening of employees is not only practical but also important for organizations to protect their digital assets. This study confirms that self-control is an individual characteristic attributable to neural structures in the right hemisphere of the brain.

This may dampen the hope of advocates of SETA (security education, training, and awareness) programs (e.g., [6, 9, 35]) in terms of effectiveness of these type of programs in information security management. This is because SETA assumes rational decision making by individuals, and if low self-control individuals are entrusted with valuable digital assets, SETA programs are unlikely to be effective in managing internal security threats originated from these individuals.

As one of the first studies that use neuroscience techniques and methodologies for investigating human decision making in the context of information security, this study inevitably has some limitations. The first is the small sample size, coupled with large variances in the ERP data, which made the statistical differences in the RFP component between the low and high self-control groups less reliable and perhaps less significant than it could be. The second is the coarse accuracy 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 the right hemisphere after onset of a decision cue, EEG data cannot pinpoint with the same precision as fMRI the specific locations in the brain where these neural processes are firing. Future study may supplement ERP data with fMRI images to provide even more refined understanding of and insight into how self-control influences decision making in information security and other social, economic, and criminological contexts.

6. Conclusion

In this study, we used brain imaging technology EEG/ERP for investigating neural correlates of human decision and self-control in the context of information security in organizational settings. Our results showed that individuals with low and high self-control activate different neural processes when making decisions related to information security policy violations, and that low self-control individuals do tend to make riskier choices that have near-term reward but significant long-term negative consequences than high self-control individuals.

Perhaps more importantly, this study established the validities of two important research instruments: an EEG/ERP paradigm for research of decision making in the context of information security, and the Grasmick et al. [14] scale as a valid measure of individual self-control. The developed EEG/ERP paradigm can serve as a foundation for future research in information security and other social, economic, and criminological studies that use scenario based stimuli. The Grasmick [14] scale can be used by researchers and managers for screening and selecting individuals based on self-control characteristics.

Hu et al. [18] have advocated screening 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.

References

[1] Antonaccio, O. and Tittle, C. R. (2008). "Morality, Self-Control, and Crime," Criminology, 46(2), 479-510.

[2] Bailey, K. M., West, R., & Anderson, C. A. (2010). "A negative association between video game experience and proactive cognitive control," Psychophysiology, 47, 34-42.

[3] Bechara, A. (2005). "Decision making, impuls control, and loss of willpower to resist drugs: a neurocognitive perspective," Nature Neuroscience, 8(11), 1458-463.

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

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

[6] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, 34(3), 523-548.

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

[8] Cunningham, W. A., Espinet, S. D., DeYoung, C. G., and Zelazo, P. D. (2005). "Attitudes to the right- and left: Frontal ERP asymmetries associated with stimulus valence and processing goals," *NeuroImage, 28*, 827-834.

[9] D'Arcy, J., Havav, A., and Galletta, D. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, 20(1), 79-98.

[10] DeLisi, M., Hochstetler, A., Higgins, G. E., Beaver, K. M., and Graeve, C. M. (2008). "Toward a General Theory of Criminal Justice: Low Self-Control and Offender Noncompliance," Criminal Justice Review, 33(2), 141-158.

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

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

[13] Gottfredson, M. and Hirschi, T. (1990). A General Theory of Crime. Stanford University Press, Stanford, CA.

[14] Grasmick, H., G. Tittle, R. Bursik Jr., and B. Arneklev. (1993). "Testing the Core Implications of Gettfredson and Hirschi's General Theory of Crime," Journal of Research in Crime and Delinquency, 30(1), 5-29.

[15] Hare, T. A., Camerer, C. F., and Rangel, A. (2009). "Self-Control in Decision-Making Involves Modulation of the vmPFC Valuation System," Science, 324(5927), 646-648.

[16] Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," MIS Quarterly, 20(3), 257-278.

[17] Higgins, G. E., Wilson, A.L., and Fell, B. D. 2005. "An Application of Deterrence Theory to Software Piracy," Journal of Criminal Justice and Popular Culture 12(3), 166-184.

[18] Hu. Q., Xu, Z. C., Dinev, T., and Ling, H. (2011) "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?" Communications of the ACM, 54(6), 34-40.

[19] Jimura, K., Chushak, M. S., and Braver, T. S. (2013). "Impulsivity and Self-Control during Intertemporal Decision Making Linked to the Neural Dynamics of Reward Value Representation," The Journal of Neuroscience, 33(1), 344-357.

[20] Johnston, A. C., and Warkentin, M. (2010). "Fear Appeals and Information Security Behaviors: An Empirical Study," MIS Quarterly, 33(4), 549-566.

[21] Kanfer, F. H. and Goldfoot, D. A. (1966). "Self-Control and Tolerance for Noxious Stimulation," Psychological Report, 18, 79-85.

[22] Knoch, D., and Fehr, E. (2007). "Resisting the Power of Temptations: The Right Prefrontal Cortex and Self-Control," Annals of the New York Academy of Sciences, 1104(1), 123-134.

[23] Malhotra, N. K., Kim, S. S., and Patil, A. (2006). "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," Management Science, 52(12), 1865–1883.

[24] Martin, L. E., and Potts, G. F. (2009). "Impulsivity in decision-making: An event-related potential investigation," Personality and Individual Differences, 46, 303-308.

[25] Mennes, M., Wouters, H., Bergh, B. V. D., Lagae, L., and Ssiers, P. (2008). "ERP correlates of complex human decision making in a gambling paradigm: Detection and resolution of conflict," Psychophysiology, 45, 714-720.

[26] Muraven, M., and Baumeister, R. F. (2000). "Self-Regulation and Depletion of Limited Resources: Does Self-Control Resemble a Muscle?" Psychological Bulletin, 126(2), 247-259.

[27] Piquero, A. and Tibbetts, S. (1996). "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), 481-510.

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

[29] Schoepfer, A. and Piquero, A. R. (2006). "Self-Control, Moral Beliefs, and Criminal Activity," Deviant Behavior, 27(1), 51-71.

[30] Seipel, C. and Eifler, S. (2010). "Opportunities, Rational Choice, and Self-Control: On the Interaction of Person and Situation in a General Theory of Crime," Crime & Delinquency, 56(2), 167-197.

[31] Siponen, M. T. and Vance, A. (2010). "Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations," MIS Quarterly, 34(3), 487-502.

[32] Symantec and Ponemon. (2009). "More Than Half of Ex-Employees Admit to Stealing Company Data According to New Study." Available at http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01

[33] Tranel, D., Bechara, A., and Denburg, N. L. (2002). "Asymmetric Functional Roles of Right and Left Ventromedial Prefrontal Cortices in Social Conduct, Decision-Making, and Emotional Processing," Cortex, 38(4), 589-612.

[34] Vazsonyi, A. T., Pickering, L. E., Junger, M., and Hessing, D. (2001). "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), 91-131.

[35] Whitman, M. E. (2003). "Enemy at the Gate: Threats to Information Security," Communications of the ACM, 46(8), 91-95.

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

[37] Wright, B. R. E., Caspi, A., Moffitt, T. E., and Paternoster, R. (2004). "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), 180-213.

[38] Zhang, L., Smith, W. W., and McDowell, W. C. (2009). "Examining Digital Piracy: Self-Control, Punishment, and Self-Efficacy," Information Resources Management Journal, 22(1), 24-44.