The Role of Rational Calculus in Controlling Individual Propensity toward Information Security Policy Non-Compliance Behavior

Qing Hu
The City University of New York
Qing.Hu@baruch.cuny.edu

Zhengchuan Xu
Fudan University
zcxu@fudan.edu.cn

Abstract

We draw on recent advances in cognitive neural science to articulate an employee security behavioral model. Cognitive neural science studies suggest two neurological processes occurring in human brain when making decisions: the automatic or reflexive process, which is the default mode for decision making, and the controlled or reflective process, which interrupts the automatic process when the brain encounters unexpected events or novel decisions. We map rational choice to the controlled process and self-control to the automatic process and test a decision model using survey data in the context of employee non-compliance behavior to organization information security policies.

1. Introduction

In the context of organizational information security management, employees inside an organization could potentially be more dangerous than those outside the organization due to their intimate knowledge about the organization's information systems and the permissions they receive either properly or improperly for their routine work activities. Numerous security breach incidents, such as the cases of Bradley Manning of US Army [15] and Edward Snowden [21], have demonstrated this point.

In organizations, information security policy violations committed by employees, or non-compliance behaviors, vary widely in motives, targets, and consequences, thus requiring a multidiscipline approach to understand and manage. Scholars have been studying this phenomenon for over two decades [5, 11, 24-25, 28-30, 53-54, 57-58], and consequently, the proposed models and theories differ significantly in terms of perspectives and prescriptions.

While prior studies have focused on different theoretical aspects of the similar focal phenomenon, we see opportunities for consolidation and integration. In addition to the possibility that different theories could potentially complement each other in providing a more comprehensive understanding of employees' information security behavior in organizational settings, we also recognize that there is at least one significant gap in the largely rational choice based behavioral research of information security: the role of individual characteristics has not been adequately addressed in the published studies and integrated into the theoretical models and frameworks in information security literature. Drawing on recent advances in neuroscience literature on human decision making processing, we proposed and test an integrated individual information security decision model aimed at a better understanding and management of employee security policy violations.

2. Theory and Hypotheses Development

2.1. Research based on rational theories

Rational choice is a normative theory of human behavior in social and economic settings. While there is not a single unified rational choice theory in the literature, it helps the discussion to articulate some fundamental concepts common to rational choice based theories. Rational choice theories can be described with five fundamental assumptions about human behavior: utility maximization, consistency, self-interest, individual centric, and stability over time and across individuals [20].

These assumptions underlie a wide range of social and economic rational theories, from criminological theories [5, 17, 43], to theories of social economic choices [6]. In the context of criminology, rational choice theory argues that the decision to engage in criminal behavior by an individual is a function of the perceived risks and benefits of committing a crime relative to the perceived risks and benefits of not committing the crime [5, 41]. This theory assumes that individuals are sensitive to the consequences of their actions and make reasoned judgments based on the risk-benefit analysis of the intended acts [52].

In the recent resurgence of information security research, deterrence theory and rational choice

URI: http://hdl.handle.net/10125/50354
ISBN: 978-0-9981331-1-9

framework continue to be the foundation of most research models. D'Arcy et al. used deterrence theory to explain information system misuse intentions of employees but found that only the severity of sanctions has a significant direct impact [11].

On the other hand, the connection between morality and behavior is also well-established in the criminological literature [1, 55]. Kohlberg's cognitive moral development (CMD) theory has been the foundation for a majority of morality based research [32]. However, criminologists are more open to the idea of cognitive morality [1]. "The cognitive morality approach assumes that the causes of behavior are not entirely confined to moral cognitions or even to conditions internal to the individual. Instead, this second approach assumes that what people actually do is influenced by a number of factors, including internal conditions (such as personality, stated moral beliefs, and psychic strains) and external conditions (such as normative expectations, potential chances of being caught and punished, and others)" [1].

Therefore, the construct of moral beliefs is often used as a proxy for the outcome of moral reasoning in the context of crime situations. For example, Piquero and Tibbetts incorporated moral beliefs into their criminal behavioral model that integrated the elements of rational choice and non-rational theories [42]. They found that moral beliefs decrease the perceived pleasure from and increase the perceived sanctions against committing criminal acts, thus reduce criminal intention.

2.2. Research based on non-rational theories

Notwithstanding their broad acceptance, rational theories have been challenged in social and economic literature [40]. Significant empirical and observational evidence of human behavior often contradicts the predictions of rational theories in a wide range of social and economic settings [18], leading to the rise of non-rational theories of human behavior.

In this study, we choose to focus on one non-rational theories commonly used in the studies of individual behavior: self-control theory. The fundamental arguments in non-rational theories are that not all human behaviours are results of ranked preferences based on deliberations of risks and benefits, as assumed in rational theories, but some are outcomes of the ability to control impulsive urge for immediate gratification or to exercise constrains based on moral values and accepted social norms about a particular situation. Decisions based on impulsive urges could be inconsistent with the predictions based on rational theories.

In criminological research, self-control theory, originated from the seminal work of Gottfredson and Hirschi, is one of the preeminent non-rational theories [16]. Instead of assuming criminal offenders contemplating their intentions or actions based on perceived risks and benefits, Gottfredson and Hirschi argued that all humans have the same potential of committing crimes given the right circumstances; however, not everyone become criminals because of individual differences in self-control – propensity to refrain from committing deviant or criminal acts under given circumstances [16]. This propensity 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.

2.3. Developing an integrated theory of non-compliance behavior

As more theories are introduced to the domain of information security research, the need for integration also increases. This is because individual theories in criminology and information security tend to focus on a primary aspect of underlying causes of a focal behavior. The goal of theory integration is to identify commonalities and complementarities in multiple theories and produce a synthesis that is superior to any of the component theories. Silberman argued for integration of deterrence theories that can accommodate recent research findings in criminological studies [51]. Cote suggested that evaluating evidence from the perspective of a single theory rarely leads to falsification of that theory and creates a major scientific challenge [10]. These critiques have resulted in the emergence of theoretical integration in criminological research in recent years [10, 39, 42, 50, 61]. Most recently, Bulgurcu et al. integrated rational choice theory as an antecedent to theory of planed behaviour [8], and Siponen and Vance integrated neutralization theory and deterrence theory into one structural model as parallel theories via direct links to non-compliance intentions [60].

Recent advances in cognitive neuroscience on human behavior suggest that individual behavior is the outcome of interactions between two basic mental processes: the controlled and the automatic processes [49]. In the controlled, or reflective, process, the brain analyzes external stimuli and makes a choice among multiple options based on established rules of behavior – moral, cultural, and economical values, as well as laws, goals, and other high level decision criteria. In the automatic, or reflexive, process, behavioral actions are triggered automatically by pre-existing

neurological and physiological conditioning in the brain of an individual over a long period of time. For instance, in the commonly used "cold pressor" test for self-control ability, a human subject is asked to put an arm into icy water for as long as he or she can bear [31]. In this type of tests, the automatic process orders the hand to pull out as soon as pain is detected, but the controlled process orders the hand to stay in the water in order to achieve some pre-set goals or outcome. In individuals with strong self-control, the controlled process will win over the automatic process and result in enduring the significant pain for extended period of time. On the other hand, in individuals with weak self-control, the automatic process will dominate over the controlled process and result in quick withdrawal to avoid suffering the pain induced by the cold water. These and other cognitive neuroscience studies suggest strong interactions between the controlled and automatic neurological processes that ultimately determine human behavior.

This brief literature review of criminology, information security, and cognitive neuroscience studies leads us to propose a research model that has both rational choice theory (which predicts controlled and reflective behavior), and non-rational theories (which predict automatic and reflexive behavior) as two parallel direct drivers of intention and behavior, while the two processes interact in the form of the controlled process (rational) moderating the automatic process (non-rational), to form a nomological network of employee non-compliance behavior toward information security policies. We submit that when an opportunity for non-compliance occurs, whether or not it arouses an individual's intention to commit the violation depends on the outcome of these two parallel processes and their interactions. This thesis leads to the formulation of the following conceptual model of information security policy non-compliance behavior of employees, as shown in Figure 1.

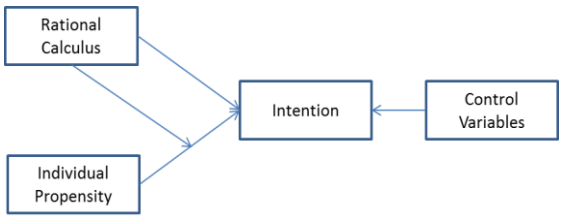


Figure 1. Conceptual Model

2.4. Developing an integrated theory of non-compliance behavior

We argue that there are at least two types of rational calculus that happen in the human brain when making social decisions: the economic calculus and the moral calculus. Both of which are generally treated as a single cost/benefit calculus in most literature based on rational choice theory. The problem with this treatment is that the cost or benefit of a decision depends on the value system used. A significantly high benefit based on economic values could have significant high cost based moral values. In this study, we differentiate these two types of calculus and theorize them as two different constructs: economic calculus in the form of deterrence and the moral calculus in the form of moral beliefs.

General deterrence theory is built on the assumption of human rationality, which makes it logical to consider integration with the other rational frameworks [17]. In this study, we submit that the effect of the deterrence on criminal behavior may be both direct and indirect, as often hypothesized in prior literature. The overall framework of rational choice theory posits that in addition to deterring criminal behavior intention by presenting certain, severe, and swift punishment, deterrence is also likely to increase the perceived risks of intended criminal act, which in turn reduces the intention to commit the criminal acts. Despite the fact that Gibbs articulated three dimensions of deterrence: certainty, severity, and celerity [17], in the literature, only the first two are usually operationalized [11, 55]. In this study, we follow the three dimension formulation of deterrence of Gibbs and argue that deterrence in general, and its components of certainty, severity, and celerity in specific, will have a significant impact on the rational calculus of an employee when considering committing information security policy violations. Hence:

H1: The stronger an individual's perceived degree of deterrence against an information security policy violation, the weaker the intention to commit the security policy violation.

Moral beliefs are defined as an individual's judgment of right and wrong about specific behavior [3]. Criminological literature suggests that morality has a direct effect in controlling criminal or deviant behavior or intention. Grasmick and Bursik argued that when an individual is contemplating doing something he or she believes is morally wrong, the sense of guilt, or shame, generated by internal conscience, serves as a form of deterrence to the behaviour [18]. There is also an argument that moral beliefs or moral commitments themselves are in effect deterrence to criminal or deviant behavior [61]. Silberman argued that "those who are already deterred from committing a deviant act because they are committed to conform to the norm cannot be deterred further by the threat of punishment" (p. 443) [51].

There is significant empirical evidence that supports a direct link between morality and behavior or behavioral intentions [56]. In a study of selected adults in Ukraine, Antonaccio and Tittle found that morality is a more important predictor of intention of criminal behavior among all factors considered, and a more potent predictor than low self-control [1]. In a recent study of adolescent criminal behavior, Wikström and Svensson found that weak morality and low self-control are two strong predictors of criminal behavior; young people with strong morality do not engage in crimes, regardless the level of self-control, suggesting a direct impact of morality on behaviour [60]. Thus, we propose:

H2: The stronger an individual's moral beliefs about information security policy violations, the weaker the intention to commit the violations.

Self-control theory has become a dominant framework for criminological inquiries [12] and has accumulated strong empirical support [42]. Self-control has been found to have direct and indirect influence on criminal behavioral intentions. In the criminology literature, the concept of self-control is operationalized as "low self-control" as a result of the widely adopted measurement developed by Grasmick et al. [19]. In this study, we use the construct "self-control" in our theorizing and Grasmick et al. instrument for measurement [19].

The extensive research based on self-control theory has provided strong empirical evidence for a direct link between self-control and deviant or criminal behavior. A large scale study of youth in four nations by Vazsonyi et al. found self-control is directly linked to a number of deviant behaviours in both genders and across different age groups, and the effects appear to be nation and culture invariant [59]. Wikström and Svensson found that when morality is low, youth with low self-control have a strong tendency to commit deviant and criminal acts [60]. Perhaps the strongest evident is the meta-analysis conducted by Pratt and Cullen that use self-control as a key predictor for criminal and "analogous" behavior (smoking, excessive drinking, driving fast, etc.) [45]. The authors found strong support for the direct role of self-control in criminal intentions. Self-control has an effect size that exceeds 0.20, which, the authors argue, puts it as one of the strongest correlates of crime when in comparison with other criminal behavior predictors reported in the literature. Langton et al. investigated the relationship between self-control and workplace theft behavior and found that attitudinal self-control as measured by Grasmick et al. [19] is the strongest predictor to workplace theft intention [34]. Given the close relationship between workplace delinquency and information security policy violations, we can logically argue that:

H3: The lower an individual's self-control, the stronger the intention to commit security policy violations.

Cognitive neuroscience literature have largely established 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. argued that self-control involves modulation by the dorsolateral prefrontal cortex (DLPFC), which is commonly known for its executive control function [37], of the value signals computed in the vmPFC [22]. They found that activity in DLPFC increased when the participants exercised self-control and correlated with activity in the vmPFC. Based on these results, Hare et al. posits that a fundamental difference between successful and failed self-control might be the extent to which the DLPFC modulates the vmPFC [22].

Lopez et al. 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 [36]. But they also found that inferior frontal gyrus (IFG), which is also associated with executive control function [2], is a critical brain region that moderates self-regulatory outcomes, especially when people are faced with strong temptations and self-control is required.

Other studies in neuroscience have found more evidence of the modulating relationships between self-control and the prefrontal cortex (PFC), especially the right PFC and the right ventromedial PFC regions [7, 33]. It is, therefore, fair to state that there is strong cognitive neuroscientific evidence to support the argument that the brain's executive control function, or the rational calculus process, moderates the effect of the reflexive function, or the self-control process, on behavior intention and actual behavior. Thus, given our previous argument that moral beliefs and deterrence are part of the rational calculus process in security policy violation behavior, we posit that:

H4: Moral beliefs negatively moderate the relationship between an individual's self-control and the intention to commit security policy violations.

H5: Deterrence negatively moderate the relationship between an individual's self-control and the intention to commit security policy violations.

2.5. Control Variables

In addition to the focal constructs, we also included two control variables in our structural model: Age and Computer Usage. Age is included because of the nominal belief that younger employees may be more prone to deviant behavior than older ones for a number of reasons. Age may have an impact on moral beliefs in the form of moral maturity [32], and age may also influence the perception of risks and benefits as older employees tend to have stronger ties with family and friends, and thus have stronger sense of obligations than younger employees [24]. Computer usage, measured as the number of hours spent on using computer at work each day, is included for one obvious reason: the more time an individual spent with computers, the more experienced and skilled the individual will become in dealing with computers, and therefore the more opportunities to commit non-compliance acts, as is suggested in routine activity theory [9].

2.6. Research Model

These discussions and research hypotheses are summarized in the research model as shown in Figure 2. The labels on the links between constructs correspond to the hypotheses developed in the previous sections.

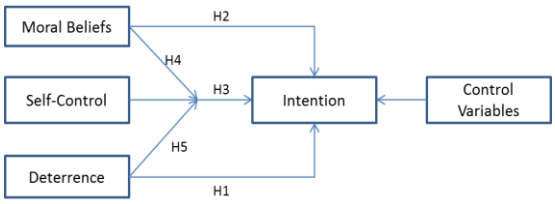


Figure 2. Research Model

3. Data and Method

This study adopted a scenario based survey strategy to collect data from employees in organizations who may or may not have committed security policy violations. The questionnaires were distributed to employees in multiple organizations where each of the randomly selected employees was asked to assess his or her intention to commit the deviant acts described in the scenario. Using scenarios to elicit individual responses has been a common technique in criminology research [3, 41-42], and it has been increasingly used by IS scholars in information security research [11, 38, 52].

We decided to strike a balance between theoretical parsimony and theoretical richness by conducting data collection using first order constructs and then testing structural models with first and second order constructs wherever theoretically justified. The second order constructs are constructed using the factor scores of the first order constructs [35, 48].

The survey instrument was developed based on the research model as shown in Figure 2. Measurement items for each latent first order construct in the model are based on a 7-point Likert scale. All of the items were adapted from the extant literature in order to maximize the validity and reliability of the measurement model. Questions related to respondent demographics and work characteristics were also included.

The instrument was first drafted in English, and then translated into Chinese by the authors who are proficient in both languages. The Chinese version was then translated back into English by the authors to check for inaccuracies. Recommended precautions were taken in designing the question items to minimize social desirability and other potential response biases [44]. The survey instrument was then pilot tested by using EMBA students enrolled in a major Chinese university in Shanghai. The data were used to run an array of statistic diagnostic tests. A number of minor modifications were made to the instrument based on the feedback from the students and the statistical characteristics of the data.

The final survey was distributed to employees in five large organizations in China. We made sure that these companies had a fairly complete set of information security policies through a telephone interview with the security managers in each company using an information security assessment framework. Primarily because of the supportive arrangement of the managers of these five organizations, the response rate of the survey was nearly 100% from about 50 randomly selected employees in each organization. The employees were assured that the management would not have access to the individual surveys. In the end, 227 surveys were received, 207 were deemed as complete and usable, 20 were discarded due to incomplete answers. 58% of the respondents are male, and 42% are female, reflecting a typical gender composition in these organizations.

4. Results and Analysis

To analyse the measurement quality as well as the path model for hypothesis testing, we used SmartPLS as the primary statistical tool, which was supplemented by SPSS for non-structural modeling statistics and tests [47]. Following the literature tradition of structural equation modeling, we first present the quality of the measurement model to show

the validity of constructs and the reliability of measurements. This is followed by structural modeling and other diagnostics testing results to show the validity and significance of the research hypotheses.

4.1. Quality of Measurement Model

The quality of the measurement model is usually assessed in terms of its content validity, construct validity, and reliability [27, 55]. Content validity is defined as the degree to which the items represent the construct being measured. Content validity is usually assessed by the domain experts and literature review [55]. In this case the content validity is primarily assured by adopting the previously published measurement items for each construct and an item by item review by the research team before and after the pilot study.

Construct validity can be assessed using convergent validity and discriminant validity. Convergent validity is shown when the t-values of the outer model loadings are statistically significant. Our results show that all item loadings for each construct are significant at $p < 0.01$ ($t > 2.576$), indicating good convergent validity. Hulland recommended that items with loading below 0.5 be dropped [27]. All item loadings in our measurement model are greater than this threshold.

Discriminant validity refers to the extent to which measures of the different model constructs are unique. There are a number of techniques that can be used to test discriminant validity [55]. In this study we assess the discriminant validity by comparing the correlations between constructs and the AVE of each construct. Discriminant validity is supported if the square root of a construct's AVE is greater than the correlations of the construct with all other constructs [13, 27]. In our case, the diagonal values in Table 1 are the square root of AVEs of the constructs, which show good discriminant validity for all constructs in the measurement model.

The reliability of the measurement addresses the concern of how well the items for one construct correlate or move together and is usually assessed by two indicators – Cronbach's alpha and composite reliability. Cronbach's alpha is a measure of internal consistency among all items used for one construct. Composite reliability addresses similar concept but is considered as a more rigorous measure in the context of structural equation modelling [46]. The lowest composite reliability is 0.797, and all but one Cronbach's alphas are higher than the recommended minimum value of 0.7 [4,14], indicating acceptable reliability of the measurement for each constructs.

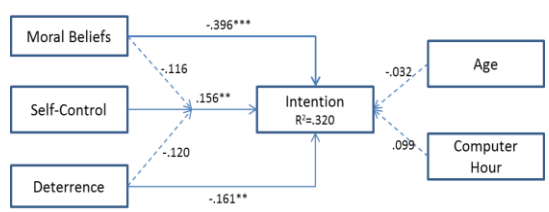
Table 1: First Order Latent Variable Correlations*

N.	Var	Mean	Std	1	2	3	4	5	6	7	8
1	CEL	5.189	1.562	.944							
2	CRT	4.939	1.562	.587	.833						
3	IMP	2.001	1.158	-.053	-.032	.816					
4	INT	1.726	1.039	-.174	-.149	.390	.763				
5	MRB	5.735	1.527	.231	.221	-.204	-.377	.800			
6	RSK	2.635	1.488	-.050	-.118	.222	.207	-.177	.838		
7	SEL	2.309	1.271	-.105	-.235	.353	.353	-.251	.508	.830	
8	SVR	5.422	1.527	.862	.585	-.017	-.169	.244	-.073	-.120	.915

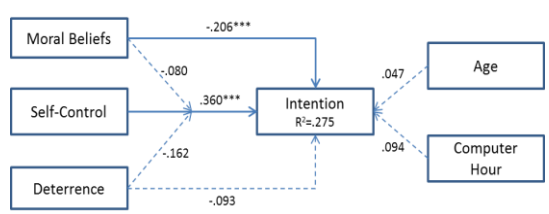
*Value in bold are square root of AVEs of the corresponding construct

4.2. Hypotheses Testing

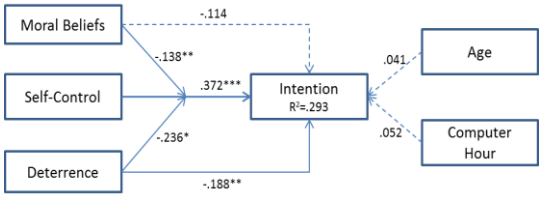
The path analysis of the structural model was carried out using SmartPLS. Since our model contains first and second order constructs, we followed the method used in Lee and Xia [35] and Ringle et al. [48] to specify the second order constructs in the structural model. We first run a model with only the first order constructs and obtained the factor scores for the formative components of the second order constructs. The standardized factor scores are then used as values of formative indicators for these second order constructs in the final structural model. Figure 3 presents the results. The path coefficients and their significance levels are shown along the paths. The moderating paths were tested using the standard procedure of SmartPLS.



(a) Scenario 1: Low Risk



(b) Scenario 2: Medium Risk



(c) Scenario 3: High Risk

Figure 3. Results of Structural Model Tests

5. Discussion

Our integrated model on employees' information security policy non-compliance behavior has been largely supported by the structural modelling results and the diagnostics tests using data collected from employees in Chinese companies. These tests have yielded a rich set of insights on why employees commit information security policy violations and what companies can do about it.

The first important finding is that the individual characteristics of self-control has a central role in shaping the intention of employees to commit security policy violations in organizations, and it is significant in all three scenarios. Interestingly, the effect of the two rational calculus constructs, moral beliefs and deterrence, on the intention of employees to commit security policy violations are mixed and dependent on the scenarios. In the low risk scenarios where unauthorized access to private information is contemplated, both moral beliefs and deterrence have significantly negative effect on the intention, and among all three constructs, moral belief has the strongest effect (β = -.396, p <.01). As the scenario changes from low risk to high risk where theft of confidential product data is contemplated, the role of self- control becomes increasing dominant (from β = -.156, p <.05, to β = -.372, p <.01), while the role of moral beliefs gradually diminishes (from β = -.396, p <.01, to β = -.114, p >.1), and the role of deterrence becomes more significant (from β = -.161, p <.05, to β = -.188, p <.05) .

The second interesting finding is that as the scenario changes from low risk to high risk, the moderating effect of the executive control function of the brain (as reflected in the rational calculus process) on the automatic reflexive function of the brain (as reflected in individual propensity operationalized as self-control) becomes stronger (from insignificant to significant).

The findings of this study contribute to the literature of information security in many areas. First, we extended the self-control theory of criminology to the information security domain and confirmed its centrality in explaining employees' non-compliance behavior in organizational context. Hypotheses related to low self-control are all strongly supported by the data. Second, we extended rational choice theory of criminology to the information security domain by showing that the theory's effectiveness in predicting human behavior is subject to individual characteristics such as self-control. Third, we believe this is the first study that have explicitly modelled self-control, moral beliefs, and deterrence as second order formative constructs in an integrated structural equation model. In doing so, we not only contributed theoretical clarity to these important constructs by creating a parsimonious theoretical model, but also provided a more refined understanding of how the components of these constructs contribute to the overall model. Fourth, our results suggest that while self-control, moral beliefs, and deterrence are all significant determinants of intention, self-control has a stronger total effect on intention than the other two, and the three constructs impact the behavioral intention in different ways.

Finally, we showed the value of theory integration when we put two opposing sets of theories about human behavior onto a seamless nomological network and produced richer results than any of the constituent theories could when used alone. By using recent findings in cognitive neuroscience as the basis for integration, we not only confirmed the validity of rational and non-rational theories in understanding human behavior, we also showed why rational choice theory may not work consistently across individuals – different individual characteristics such as self-control could significant alter the outcome of rational analysis in any given situation. This may also help explain the inconsistent findings in the literature about the effect of deterrence [11, 23, 25, 53-54].

We must acknowledge that this study has a number of limitations. First and foremost, the data came from a pseudorandom sample of five organizations. The five organizations were selected from a large pool of organizations the authors contacted based on their willingness to participate. A true random sample of a larger number of organizations might yield much stronger and convincing results. Second, the characteristics of the respondents, especially the dominance of the younger employees in the pool and the fact that they were all from China where national and organizational cultures could be unique, may limit the generalizability of some of the findings. A comparative study with employees from different cultures and countries might complement the findings of this study and provide better understanding of employees' behavior. Third, while using second order

constructs accomplishes the objective of theoretical parsimony when integrating multiple theories, it does result in loss of information and intricate relationships among the first order constructs implied by the research model. It is not feasible to fully develop the first order model in this study, but future research could focus on testing the significant relationships identified. Fourth, there are many other rational and non-rational theories that have been used for studying employees' compliance behavior, including protection motivation [23], neutralization [53], and fear [28]. It is certainly interesting to explore how some of these factors impact the basic framework of rational choice in the context of information security policy compliance/non-compliance. Finally, our structural models only show the linkage between the rational and non-rational processes based on aggregated survey data. The partial mediation by the rational constructs on the effects of non-rational constructs suggests that it is possible in some individuals, such as those with strong moral beliefs or weak self-control, that the rational process may not even be activated in specific situations. The recent advance in cognitive neuroscience research could help design future studies with controlled experiment and sophisticated neurophysiological and neuroimaging measures to advance our knowledge in this regard.

6. Conclusion

In this paper, we developed and tested a model of information security policy violations by employees in organizational settings by integrating two opposing theoretical paradigms – rational vs. non-rational theories of human behavior based on recent findings in cognitive neuroscience. We found that rational choice theory of deviant behavior is largely supported. However, the most interesting findings are that the personal characteristics of low self-control has a central role in explaining employees' intention to commit information security policy violations inside organizations. In addition, we found that deterrence and moral beliefs influence the rational calculus differently in different scenarios, and the rational processes indeed have a strong moderating effect on the non-rational calculus but only in high risk scenarios.

7. Acknowledgement

This research is supported in part by the National Natural Science Foundation of China (71772042, 71272076; 71429001).

8. References

[1] Antonaccio, O., and Tittle, C. R. "Morality, Self-Control, and Crime," Criminology (46:2), 2008. pp. 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. pp.170-177.

[3] Bachman, R., Paternoster, R., and Ward, S. "The Rationality of Sexual Offending: Testing a Deterrence/Rational Choice Conception of Sexual Assault," Law & Society Review, (26:2), 1992. pp.343-372.

[4] Bagozzi, R. P. and Yi, Y. "On the Evaluation of Structural Equation Models," Journal of the Academy of Marketing Science, (16:1), 1988. pp. 74-94.

[5] Becker, G. S. "Crime and Punishment: An Economic Approach," Journal of Political Economy (76:2), 1968. pp.169-217.

[6] Becker, G. S. The Economic Approach to Human Behavior, Chicago and London: The University of Chicago Press. 1976.

[7] 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 & Affective Neuroscience, 4, 1, 2009. pp. 1-9.

[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. pp.523-548.

[9] Cohen, L. E., and Felson, M. "Social Change and Crime Rate Trends: A Routine Activity Approach," American Sociological Review (44:4), 1979. pp.588-608.

[10] Cote, S. Introduction, in Criminological Theories – Bridging the Past to the Future, Cote, S. (Eds.), Sage Publications, Thousand Oaks, CA. 2002.

[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. pp.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. pp. 141-158.

[13] Fornell, C. and Larcker, D. F. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research (18), 1981. pp.39-50.

[14] Gefen, D., Straub, D. W., Boudreau, M. C. "Structural Equation Modeling And Regression: Guidelines for Research Practice," Communications of AIS (4), 2000. Article 7.
[15] Gerstein, J. "Bradley Manning's WikiLeaks case: The larger issue," Politico, available at http://www.politico.com/news/stories/1211/70826.html. 2011.
[16] Gottfredson, M. and Hirschi. T. A General Theory of Crime, Stanford University Press, Stanford, CA. 1990.
[17] Gibbs, J. P. Crime, Punishment, and Deterrence, Elsevier, New York. 1975.
[18] Grasmick, H.G., and Bursik, R.J. "Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model," Law and Society Review (24:3), 1990. pp.837-861.
[19] Grasmick, H., Tittle, C. R., Bursik Jr., R. J., 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. pp. 5- 29.
[20] Green, D. P., and Shapiro, I. Pathologies of Rational Choice Theory: A Critique of Applications in Political Science, New Heaven and London: Yale University Press. 1994.
[21] Harding, L. How Edward Snowden went from loyal NSA contractor to whistleblower, The Guardian, available at https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract. 2014.
[22] 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. pp. 646-648.
[23] Herath, T., and Rao, H. R. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations" European Journal of Information Systems(18:2), 2009. pp.106–125.
[24] Hirschi, T. Causes of Delinquency, Berkeley, CA: University of California Press. 1969.
[25] Hu, Q., Xu, Z., Dinev, T., and Ling, H. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?" Communications of the ACM (56:4), 2011. pp.34-40.
[26] Hu, Q., Dinev, T., Hart, P., and Cooke, D. "Managing Employee Compliance with Information Security Policies: The Role of Top Management and Organizational Culture," Deci-sion Sciences (43:4), 2012. pp. 615-660.
[27] Hulland, J. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Re-view of Four Recent Studies," Strategic Management Journal (20), 1999. pp.195–204.
[28] Johnston, A. C., and Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study," MIS Quarterly (33:4), 2010. pp.549-566.
[29] Johnston, A. C., Warkentin, M., and Siponen, M. "An Enhanced Fear Appeal Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," MIS Quarterly (39:1), 2015. pp. 113-134.
[30] Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. D. "Dispositional and Situational Factors: Influences on IS Security Policy Violations," European Journal of Information Systems (25:3), 2016. pp. 231-251.
[31] Kanfer, F.H., and Goldfoot, D.A. "Self-control and tolerance for noxious stimulation", Psychological Report, 18, 1966. pp. 79–85.
[32] Kohlberg, L. The Philosophy of Moral Development. San Francisco: Harper & Row. 1981.
[33] Knoch, D. and Fehr, E. "Resisting the power of temptations," Annals of the New York Academy of Sciences, 1104(1), 2007. pp. 123-134.
[34] Langton, L., Piquero, N. L., and Hollinger, R. C. "An Empirical Test of the Relationship between Employee Theft and Low Self-Control," Deviant Behavior (27:5), 2006. pp. 537-565.
[35] Lee, G., and Xia, W. "Toward Agile: An Integrated Analysis of Quantitative and Qualitative Field Data on Software Development Agility," MIS Quarterly (34:1), 2010. pp.87-114.
[36] 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. pp. 1337-1344.
[37] Miller, E. K., & Cohen, J. D. "An integrative theory of prefrontal cortex function," Annual review of neuroscience, 24(1), 2001. pp. 167-202.
[38] Moores, T. T. and Chang, J. C. "Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model," MIS Quarterly (30:1), 2006. pp.167-180.
[39] Nagin, D.S., and Paternoster, R. "Personal Capital and Social Control: The Deterrence Implications of a Theory of Individual Differences in Criminal Offending," Criminology (32:4), 1994. pp. 581–606.
[40] Parisi, F., and Smith, V. L. (Eds.). The Law and Economics of Irrational Behavior, Stan-ford, CA: Stanford University Press. 2005.
[41] Paternoster, R. and Simpson, S. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," Law & Society Review (30:3), 1996. pp.549-583.
[42] 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. pp.481-510.
[43] Piquero, A., and Tibbetts, S. Rational Choice and Criminal Behavior: Recent Re-search and Future Challenges, New York, NY: Routledge. 2002.
[44] Podsakoff, P. M., and Organ, D. W. "Self-Reports in Organizational Research: Problems and Prospects," Journal of Management (12:4), 1986. pp.531– 543.
[45] Pratt, T. C., and Cullen, F. T. "The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis," Criminology (38:3), 2000. pp.931-964.
[46] Raykov, T. "Coefficient Alpha and Composite Reliability with Interrelated Nonhomogeneous Items," Applied Psychological Measurement (22:4), 1998. pp.375-385.
[47] Ringle, C. M., Wende, S., and Will, A. SmartPLS, 2.0 (beta), University of Hamburg, Hamburg, Germany, available on the Web at http://www.smartpls.de. 2005.
[48] Ringle, C.M., Sarstedt, M., Straub, D.W. "A critical look at the use of PLS-SEM in MIS quarterly," MIS Quarterly 36 (1), 2012. pp. iii-xiv
[49] Satpute, A. B., and Lieberman, M. D. "Integrating automatic and controlled processes into neurocognitive models of social cognition," Brain Research, 1079(1), 2006. pp. 86-97
[50] 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 & Delinquency, (56:2), 2010. pp. 167-197.
[51] Silberman, M. "Toward a Theory of Criminal Deterrence," American Sociological Review (41:3), 1976. pp. 442-461.
[52] Simpson, S. S., and Piquero, N. L. "Low Self-Control, Organizational Theory, and Corporate Crime," Law & Society Review (36:3), 2002. pp. 509-548.
[53] Siponen, M. T. and Vance, A. "Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations," MIS Quarterly (34:3), 2010. pp. 87-502.
[54] Straub, D. W. "Effective IS Security: An Empirical Study," Information Systems Research (1:3), 1990. pp.255-276.
[55] Straub, D. W., Boudreau, M. C., and Gefen, D. "Validation Guidelines for IS Positivist Research," Communications of the AIS (13), 2004. pp.380-427.
[56] Trevino, L. K. "Moral Reasoning and Business Ethics: Implications for Research, Education, and Management," Journal of Business Ethics (11:5/6), 1992. pp.445-459.
[57] Vance, A., Lowry, P.B., Eggett, D. "Using Accountability to Reduce Access Policy Violations in Information Systems," Journal of Management Information Systems (29:4), 2013. pp. 263–289.
[58] Vance, A., Lowry, P.B., Eggett, D. "Increasing Accountability through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations." MIS Quarterly (39:2), 2015. pp. 345–366.
[59] 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. pp.91-131.
[60] Wikström, P. H., and Svensson, R. "When Does Self-Control Matter? The Interaction be-tween Morality and Self-Control in Crime Causation," European Journal of Criminology (7:5), 2010. pp.395-410.
[61] 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. pp.180-213.