7-2010

Why Individuals Commit Computer Offences in Organizations: Investigating the Roles of Rational Choice, Self-Control, and Deterrence

Qing Hu
Iowa State University, qinghu@iastate.edu

Zhengchuan Xu
Fudan University

Tamara Dinev
Florida Atlantic University

Hong Ling
Fudan University

Why Individuals Commit Computer Offences in Organizations: Investigating the Roles of Rational Choice, Self-Control, and Deterrence

Abstract
Computer offences and crimes against corporate computer systems have increasingly become a major challenge to information security management in the Internet-enabled global economy and society. In this study, we attempt to develop a theoretical model that integrates three main stream criminology theories, i.e., general deterrence, rational choice, and individual propensity. We submit that, while the main decision process leading to an offensive act may be explained by the rational choice theory, self-control and deterrence factors could significantly alter the risk-benefit calculus assumed in the rational choice model. Using data collected from employees in multiple organizations, we tested our model using structural equation modelling techniques. We found that the perceived benefits of offensive acts dominate the rational calculus in individuals, and that the low self-control significantly impacts the perceived benefits and risks, thus playing a major role in the computer offences perpetrated by individuals in organizational settings. In addition, we found that deterrence only has limited impact on the offensive intentions through increased perceived risks. By integrating multiple theories into one seamless model, we hope to provide better understanding of computer offences and deeper insights for improving information security management practices.

Keywords
Information Security, Criminology, Individual Behavior, Computer Crimes, Computer Offences

Disciplines
Information Security | Management Information Systems

WHY INDIVIDUALS COMMIT COMPUTER OFFENCES IN ORGANIZATIONS: INVESTIGATING THE ROLES OF RATIONAL CHOICE, SELF-CONTROL, AND DETERRENCE

Qing Hu, College of Business, Iowa State University, Ames, IA, USA, qinghu@iastate.edu

Zhengchuan Xu, School of Management, Fudan University, Shanghai, China, zcxu@fudan.edu.cn

Tamara Dinev, College of Business, Florida Atlantic University, Boca Raton, FL, USA, tdinev@fau.edu

Hong Ling, School of Management, Fudan University, Shanghai, China, hling@fudan.edu.cn

Abstract

Computer offences and crimes against corporate computer systems have increasingly become a major challenge to information security management in the Internet-enabled global economy and society. In this study, we attempt to develop a theoretical model that integrates three main stream criminology theories, i.e., general deterrence, rational choice, and individual propensity. We submit that, while the main decision process leading to an offensive act may be explained by the rational choice theory, self-control and deterrence factors could significantly alter the risk-benefit calculus assumed in the rational choice model. Using data collected from employees in multiple organizations, we tested our model using structural equation modelling techniques. We found that the perceived benefits of offensive acts dominate the rational calculus in individuals, and that the low self-control significantly impacts the perceived benefits and risks, thus playing a major role in the computer offences perpetrated by individuals in organizational settings. In addition, we found that deterrence only has limited impact on the offensive intentions through increased perceived risks. By integrating multiple theories into one seamless model, we hope to provide better understanding of computer offences and deeper insights for improving information security management practices.

Keywords: Information Security, Criminology, Individual Behavior, Computer Crimes, Computer Offences.

1 INTRODUCTION

Managing information security in organizations is to a large degree managing human behavior in the organizations. In a recent survey of IT mangers 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 viruses, Trojan horse, and Internet worms, (Ernst & Young, 2008). Understanding why employees commit misconducts or even criminal acts against organizational IT systems is the most important first step towards effective information security management. To this end, the majority of the information security literature has been devoted to the human behavior aspect of information security based on various theoretical lenses. Since computer offences and employee misconducts against information systems are closely related to criminal behavior, IS scholars have naturally been attracted to the literature of criminology. For example, general deterrence theory (GDT) has been used by Straub (1990), Straub and Welke (1998), and D'Arcy et al. (2009) as the foundation to understand employee misconducts in organizations. Similarly, Willison (2006) and Willison and Backhouse (2006) have developed frameworks based on rational choice and situational crime prevention perspectives for understanding computer crimes and employee misconducts and developing preventive measures and systems in organizational settings. On the other hand, from the behavioral modification perspective, Dinev and Hu (2007) have proposed an individual security behavior model based on the theory of planned behavior (Ajzen, 2002) for understanding employee security behavior and developing organizational and national policies for effective information security management.

These models and theories differ significantly in terms of perspectives and prescriptions. In addition to the possibility that they could potentially complement each other in providing a more comprehensive understanding of human behavior in organizational information security settings, we also recognize that there is at least one significant gap in the behavioral research of information security: the role of the stable individual traits has been missing from these models and frameworks, that is, the individual propensity towards committing criminal or offensive acts. The individual propensity theory, also known as social control theory, originated from the seminal work of Gottfredson and Hirschi (1990) about a general theory of crime. This theory posits that individual difference (or propensity) predisposes an individual to criminal behavior. However, one critical question that remains is how the individual propensity interacts with other known factors in criminology, such as deterrence, rational choice, crime situation, and other individual and organizational factors commonly identified in the organizational information security literature.

In this study, we set out to extend the current research on the behavioral aspects of information security and attempt to accomplish the following three objectives: 1) integrate multiple theories to develop a theoretical model about computer offensive behavior in corporate settings, 2) test the relationships among rational choice, deterrence, individual propensity, and computer offensive outcome of individuals, and 3) provide prescriptive guidance to information security management based on the results from the empirical testing of the theoretical model. Corporate computer offences and computer crimes vary widely in motives, forms, targets, and consequences. In this study, we focus on internal computer offence defined as any act by an employee using computers that is against the established rules and policies of an organization. By this definition, computer offences include but are not limited to unauthorized access to data and systems, unauthorized copying or transferring of confidential data, or selling confidential data to third party for personal gains, etc.

The rest of the paper is arranged as follows. We first review the relevant literature and provide a brief description of each of the theories used in the study. This is followed by presenting our integrated research model from which we developed our research hypotheses. We then proceed to discussing the research design and methodology. Finally, we present the results of the empirical testing of the model and discuss the contributions of this study and the potential implications for theory and practice.

2 THEORETICAL DEVELOPMENT

The significant role of human agents in organizational information security has long been recognized by scholars, along with the effort in developing and deploying more advanced protective technologies and establishing and enforcing effective security policies and procedures. Early studies of information security by IS scholars were largely based on surveys of managers and employees in organizations using ad hoc theoretical or empirical frameworks (e.g., Goodhue and Straub 1991; Loch et al. 1992). Recently IS scholars started to use more established theories in their analyses of the information security issues (e.g., Kankanhalli et al. 2003; Dinev and Hu 2007; Boss et al., 2009, D'Arcy et al. 2009). Given the similarity between computer offences and misconducts in organizational settings and criminal behavior in social settings, the theories developed in the criminology literature have been adopted as the mainstream foundations for information security research, including but not limited to general deterrence theory, rational choice theory, and social control theory. Willison and Backhouse (2006) provided a detailed discussion on many of these theoretical perspectives.

The existence of a large number of theories, each taking a different perspective on criminal behavior, creates opportunities for developing integrated models and theories. However, how exactly these theories should be integrated into one integrated criminal behavior model is far from clear. Piquero and Tibbetts (2002) proposed a model in which the effects of individual propensity variables (prior offending, moral beliefs, and low self-control) on the criminal behavior intention are mediated by the rational choice variables (perceived benefits, perceived cost, and situational shame). On the other hand, Paternoster and Simpson (1996) found that when the moral inhibitions were high, an individual's consideration of costs and benefits of corporate crime were virtually superfluous; when the moral inhibitions were weak, however, the individual was more likely to be deterred by threats of formal and informal sanctions and by the organizational context.

The literature reviews of both criminology and information security studies lead us to propose a research model that has the rational choice at its core and other theoretical frameworks at its peripheral to form a nomological network of computer offensive behavior. We submit that when an opportunity to commit a computer crime exists, whether or not an individual commits the crime depends on the rational calculus of costs and benefits of the intended act by the individual. However, the mechanisms of the cost-benefit calculus are affected by two independent forces: one internal and one external to the individual. The internal force is the individual propensity, defined as the degree of low self-control (Gottfredson and Hirschi 1990). The external force is the general deterrence related to committing the offensive act, defined as the perceived certainty, severity, and celerity of sanction against the behavior (Gibbs 1975). We argue that low self-control and deterreance are antecedents of the rational choice calculus. This is because we believe that these internal and external factors are more likely to change how the benefits and risks are assessed by the individual rather than how much the individual weighs the benefits or risks in the decision calculus. In the sections that follow, we develop this model and its hypotheses based on the extant literature via a deductive process.

2.1 Rational Choice Theory of Criminal Behavior

The rational choice theory of criminal behavior argues that the decision to engage in criminal behavior by an individual is a function of the perceived costs and benefits of the crime relative to the perceived costs and benefits associated with non-crime (Becker 1968; Cornish and Clarke 1986; Paternoster and Simpson 1996). Although this theory has been criticized by some criminologists (Akers 1990), studies have found strong empirical evidence that supports the basic arguments of the theory. For example, Nagin and Paternoster (1993) investigated the criminal behavior (theft, drinking and driving, and sexual assault) using college students and found that conditions pertaining to rational choices must be included in the model in order to account for the amount of variances in observed criminal behavior.

In this study, we submit that computer offence is a type of deviant behavior which has more or less similar incentives and consequences as other types of deviant behavior such as crimes. Like crimes, committing computer offences generate extrinsic benefits (money, material) and intrinsic benefits

(thrill, happiness), and formal risks (legal and monetary sanctions) and informal risks (loss of respect, loss of support) (Buchman et al. 1992) simultaneously to the perpetrator. Therefore, the rational choice arguments of criminology can be naturally extended to explain the decisions pertaining to the computer offences. Thus, we propose:

H1a: The higher an individual's perceived extrinsic benefits from the offensive act, the stronger his or her intention to commit the computer offense.

H1b: The higher an individual's perceived intrinsic benefits from the offensive act, the stronger his or her intention to commit the computer offense.

H1c: The higher an individual's perceived risk of formal sanction against the offensive act, the weaker his or her intention to commit the computer offense.

H1d: The higher an individual's perceived risk of informal sanction against to the offensive act, the weaker his or her intention to commit the computer offense.

2.2 Self-Control Theory of Criminal Behavior

The self-control theory originated from the seminal work of Gottfredson and Hirschi (1990) in an attempt to develop a general theory of crime. They argued that all human beings have the same potential of committing crimes given the right circumstances. However, not everyone becomes a criminal and the reason is the individual differences in self-control – propensity to refrain from committing criminal acts under any circumstance. This propensity is said to be established early and remains relatively stable throughout an individual's life (Gottfredson and Hirschi 1990). Criminal behavior is likely to occur when individuals with low self-control are presented with opportunities for committing crimes.

The self-control theory and the rational choice theory are built on the same basic assumption, that human beings are rational in their decision making processes. This makes the integration of the two frameworks logical. It can be argued that the two theories are looking into criminal behavior from different perspectives: the stable personal characteristics vs. the dynamic calculus process. We argue that personal characteristics such as low self-control affect an individual's ability to evaluate the benefits and risks in a systematic manner. The immediate gratification and thrill seeking are the trade-mark characteristics of low self-control, which will likely result in overestimating the benefits of the criminal act, and underestimating the potential risks. Thus, we propose that:

H2a: The lower an individual's self-control, the higher the perceived extrinsic benefits of the computer offense.

H2b: The lower an individual's self-control, the higher the perceived intrinsic benefits of the computer offense.

H2c: The lower an individual's self-control, the lower the perceived risks of informal sanctions against the computer offense.

H2d: The lower an individual's self-control, the lower the perceived risks of formal sanctions against the computer offense.

2.3 General Deterrence Theory of Criminal Behavior

Human society has long recognized the role of deterrence in preventing criminal behavior. In fact, the foundation of the modern justice system in most civilized societies is largely based on the utilitarian philosophy behind the deterrence theory of crime (Akers 1999, p. 15). The general deterrence theory (Gibbs 1975) argues that an individual is less likely to commit criminal acts if the perceived certainty, severity, and celerity of the sanctions against the acts are greater. Subsequent research in criminology and social studies has established general support for this framework (e.g., Tittle 1980; Nagin and Pogarsky 2001). Deterrence theory is also the first criminology framework to be used by IS scholars for studying information security issues (e.g. Straub 1990; Staub and Nance 1990; D'Arcy et al. 2009).

Similar to self-control theory, general deterrence theory is also built on the same assumption of human rationality, which makes it logical to consider integration with the other two frameworks. In this study, we argue that the effect of the deterrence on criminal behavior may not be direct, as often hypothesized in prior literature. Instead, in the overall framework of rational choice theory, the role of deterrence is more likely in increasing the perceived risks and decreasing the perceived benefits of the intended criminal act, which in turn reduce the intention to commit the crime. This logic should apply to computer offences as well. Hence:

H3a: The stronger the perceived deterrence, the lower the perceived extrinsic benefits of the computer offence.

H3b: The stronger the perceived deterrence, the higher the perceived intrinsic benefits of the computer offence.

H3c: The stronger the perceived deterrence, the higher the perceived risks of informal sanction against the computer offence.

H3d: The stronger the perceived deterrence, the higher the perceived risks of formal sanction against the computer offence.

2.4 An Integrated Theory of Criminal Behavior

The research hypotheses developed in the above sections can be summarized in one integrated model of computer offensive behavior, as shown in Figure 1. In addition to the constructs and relationships discussed, this model also includes two control variables: age and computer use. Age is included because it is commonly used in criminological and information security studies as a control variable. We included computer use, measured as the average hours of using computers by an employee to control for the effect of difference level of access to computer systems and user computer skills.

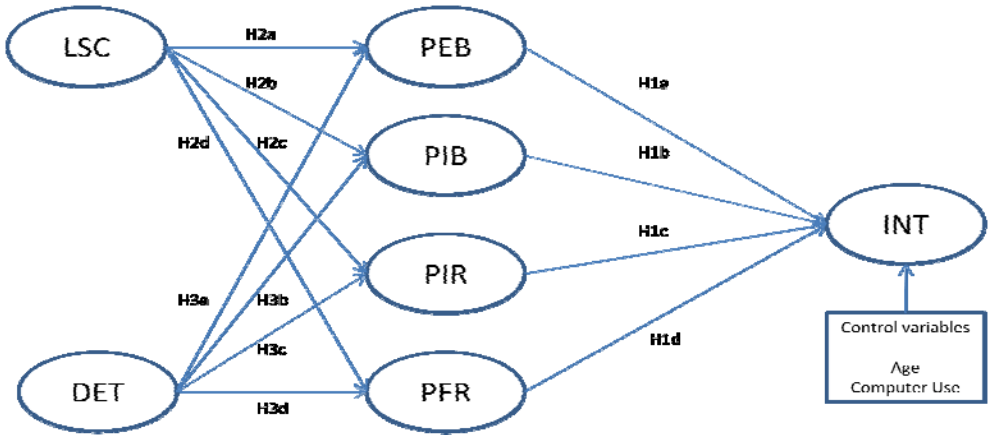

Figure 1: Research Model

(LSC-low self control, DET-deterrence, PEB-perceived extrinsic benefits, PIB-perceived intrinsic benefits, PIR-perceived informal risks, PFR-perceived formal risks, INT-intention to commit computer offence)

In the following sections, we discuss how this theoretical model is tested using data collected from individuals in different organizations and present the analysis of the results using structural equation modelling techniques.

3 DATA AND METHOD

3.1 Research Design

This study adopted a scenario based survey strategy to collect data from employees in organizations who may or may not have committed offensive acts towards corporate computers and systems. The questionnaires were distributed to employees in multiple organizations where each randomly selected

employee will be asked to assess his or her intention to commit the offensive acts described in the three scenarios with varying levels of severity of offence.

Using scenarios to elicit individual responses has been a common technique in criminology research (e.g., Batchman et al. 1992; Paternoster and Simpson 1996; Piquero and Tibbetts 1996), and it has been increasingly used by IS scholars in information security research (e.g., Harrington 1996; Moores and Chang 2006, and D'Arcy et al. 2009). Due to the secrecy associated with criminal or illicit behavior, it is natural that individuals will be unwilling or uncomfortable to report their own actions related to computer offences or crimes, not to mention knowing their peers' offensive activities. Therefore, the questionnaires commonly used in information security research that rely on self-reporting of illicit or criminal behavior might not be reliable. In criminological research, faced with the same difficulty, scholars have often resorted to the use of scenarios of criminal activities to elicit input from survey subjects. Since these scenarios describe fictitious situations and the respondents are asked what they "could" or "would" do under the same or similar situations, rather then what they "did" or "have done", the pressure to tell lies is less, thus more reliable responses are more likely.

3.2 Operationalization of Constructs

Intention to offend (INT). Intention to offend is measured as a reflective construct in different scenarios by asking the respondent "how likely," and "how willing" the respondent would do what the factious character did in the specific scenarios. This is different from the commonly used approach in the literature (e.g., Piquero and Tibbetts 1996) where only one question is used for the likelihood the subject would perform the behavior described in the scenarios. We use two items with slight variations to increase the reliability of the measurement. This measure is repeated for the three scenarios, resulting in a total of six items for the construct.

Low self-control (LSC). Grasmick et al. (1993) operationalized low self-control into six components: impulsivity, preference to simple tasks, risk seeking, preference to physical activity, self-centered, and volatile temper. In order to control the length of the measurement instrument based on the characteristics of the focal offending behavior (computer offense), for this study we adopted three of these components – impulsivity, risk seeking, and self-centered with their associated measures.

Perceived extrinsic benefits (PEB). This construct is modelled as a reflective construct primarily focusing on the perceived material benefits by the individual who commits the offending behavior. The items were constructed partially based on the items in Paternoster and Simpson (1993).

Perceived intrinsic benefits (PIB). This construct is modelled as a reflective construct primarily focusing on the perceived pleasure and fun by the individual who commits the offending behavior. The items were constructed partially based on the items in Paternoster and Simpson (1993).

Perceived risk of formal sanction (PFR). This construct is modelled as a reflective construct primarily focusing on the perceived risk of two formal sanctions - lose of job and legal actions - by the individual who commits the offending act. Risk is measured by the product of the probability and the severity of the sanction. The measurement is modelled after Buchman et al. (1992).

Perceived risk of informal sanction (PIR). This construct is modelled as a reflective construct primarily focusing on the perceived risk of two informal sanctions – loss of respect from family and relatives and loss of respect from friends and colleagues - by the individual who commits the offending behavior. Risk is measured by the product of the probability and the severity of the sanction. The measurement is modelled after Buchman et al. (1992).

Deterrence (DET). In criminological literature, the construct of deterrence is often operationalized into three first order constructs: certainty of sanction, severity of sanction, and celerity of sanction (Gibbs 1975; Antia et al. 2006). Each of the first order constructs was measured using three reflective items. However, to simplify the model and gain theoretical parsimony, we constructed the deterrence construct as a reflective second order construct with all nine items from the first-order constructs. One item was later removed from the model due to low item loading.

3.3 Survey Development and Data Collection

The measurement items for each 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. Three carefully designed computer offence scenarios are presented to each respondent at the beginning of the survey to elicit their assessment of intention to do the same as the actor did in each of the scenarios. The offensive scenarios include unauthorized access to payroll data, unauthorized access and transfer of product design, and stealing and selling price and cost data to competitors.

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. Numerous changes were made to the original versions until the authors all agreed that the items accurately reflect the intention of the measurement. The survey instrument was then pilot tested using EMBA students enrolled in a top Chinese university in Shanghai. A total of 31 valid responses were received, along with oral comments from the students. The data were used to run an array of diagnostic tests. A number of 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 organizations in China. These organizations were selected largely due to their willingness to cooperate with this research after the authors contacted a number of organizations. Primarily due to the strong support of the managers in these five organizations, the response rate of the survey is nearly 100% from the 50 randomly selected employees in each organization. In the end, 227 surveys were received, and 207 were deemed as complete and usable. The demographic profile of the respondents is described in Table 2.

Category	Measures	Frequency	Percentage (%)
Age	< 24	45	21.74
	25 – 34	119	57.49
	35-44	29	14.01
	44-55	10	4.83
	> 55	3	1.45
Sex	Male	119	57.47
	Female	87	42.03
Education	High school	2	0.97
	Professional School	55	26.57
	Undergraduate	101	48.79
	Graduate	44	21.26
	Doctoral	3	1.45
Job Title	Manager	12	5.80
	Supervisor	19	9.18
	Team leader	8	3.87
	Director	2	0.97
	Employee	156	75.36
	Other	9	4.35
Job Type	Administrative	35	16.91
	Operational	53	25.60
	Technical	45	21.74
	Professional staff	27	13.04
	Other	44	21.26

Table 2: Demographic Profile of Respondents

4 RESULTS

To analyze the measurement quality as well as the path model for hypothesis testing, we used SmartPLS (Ringle et al. 2005) as the primary statistical tool. Following the widely adopted two-step approach to structural equation modelling (Anderson and Gerbing 1988; Hulland 1999), we first assessed the quality of the measurement model to ensure the validity of constructs and reliability of

the measurements. This is followed by structural modelling to test the research hypothesis and the overall quality of the proposed model.

4.1 Quality of Measurement Model

Assessment of the measurement model's quality is the critical first step toward structural equation modelling analysis. Ideally, the quality of the measurement model should be assessed using model fit indices such as χ^2 provided by CFA analysis. However, due to the differences in underlying assumptions about data characteristics, component based SEM techniques such SmartPLS does not provide the fit indices. On the other hand, it does provide a rich set of indicators about reliability and convergent and discriminant validity. Table 3 shows some of the quality indicators of our measurement model.

Latent Construct	No. of Items	Item Loading (t-stats)	AVE	Composite reliability	Cronbach's Alpha
DET	8	0.728(15.393),0.707(11.596),0.900(45.781),0.858(22.892), 0.813(16.524),0.887(30.061),0.864(26.533),0.867(24.917)	0.6922	0.9470	0.9353
INT	6	0.654(8.539),0.841(20.522),0.858(27.650),0.577(7.794), 0.771(11.601),0.792(15.469)	0.5825	0.8919	0.8527
LSC	6	0.594(4.908),0.557(5.609),0.776(10.993),0.696(8.536), 0.700(9.183),0.697(9.925)	0.4611	0.8353	0.7635
PEB	3	0.936(37.049),0.950(14.364),0.926(15.396)	0.8892	0.9601	0.9382
PFR	2	0.866(24.716),0.920(56.575)	0.8016	0.8898	0.7553
PIB	3	0.886(24.660),0.934(40.619),0.878(23.327)	0.8112	0.9279	0.8831
PIR	2	0.931(60.292),0.916(38.164)	0.8529	0.9206	0.8279

Table 3: Measurement Quality Indicators

The quality of the measurement model is usually assessed in terms of its content validity, construct validity, and reliability (Hulland 1999; Straub et al. 2004). 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 (Straub et al. 2004). In this case the content validity is primarily assured by adopting the previously published measurement items for the construct and an item by item review by the research team.

Construct validity can be assessed using convergent validity and discriminant validity. Convergent validity is defined as the degree to which the measurement items are related to the construct they are theoretically predicted to be related. Convergent validity is shown when the t-values of the outer model loadings are statistically significant. As it can be seen from Table 3, all item loadings for each construct are significant at $p < 0.01$ ($t > 2.576$), indicating good convergent validity. Hulland (1999) recommends that items with loading below 0.5 should be dropped. 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 have been used to for testing discriminant validity in the literature (Straub et al. 2004). In this study we assess the discriminant validity by comparing the correlations between constructs and the AVE of each construct. This is a widely used technique in the IS literature when component based SEM methods such as PLS is used. Discriminant validity is supported if the square root of construct AVE is greater than the correlations of the construct with all other constructs (Fornell and Larcker 1981; Hulland 1999). In our case, the diagonal values in Table 4 are AVEs of constructs, which show good discriminant validity for all constructs in the measurement model.

	DET	INT	LSC	PEB	PFR	PIB	PIR
DET	**0.6922**						
INT	-0.2127	**0.5825**					
LSC	-0.1293	0.4656	**0.4611**				
PEB	-0.1295	0.2409	0.1441	**0.8892**			
PFR	0.3668	-0.3279	-0.2974	-0.088	**0.8016**		

PIB	-0.1522	0.4732	0.4392	0.2096	-0.372	**0.8112**	
PIR	0.3112	-0.4195	-0.3233	-0.0853	0.5838	-0.3151	**0.8529**

Table 4: Latent Variable Correlations (values on the diagonal are AVEs)

The reliability of the measurement addresses the concern of how well the items for one construct correlate or move together (Straub et al. 2004). Reliability is usually assessed by two indicators – Cronbach's apha and composite reliability. Cronbach's alpha is a measure of the internal consistency among all items used for one construct. Composite reliability addresses similar concept but is considered as a more rigorous reliability measure in the context of structural equation modelling (Raykov 1998; Chin 1998). The reliability indicators of the constructs in this study are shown in Table 3. The lowest composite reliability is .0.83 and the lowest Cronbach's alpha is 0.75, higher than the recommended minimum value of 0.7 (Baggozzi and Yi 1988; Gefen et al. 2000), indicating acceptable reliability of the measurement for each constructs.

4.2 Structural Analysis

Component based PLS techniques do not provide overall model fit indices. The primary indicators for the quality of the structural model are the R^2 values of the endogenous variables (Hulland 1999), which measure how much of the variances in the endogenous constructs are explained by the exogenous constructs specified in the model. Figure 2 presents the results of the structural analysis using SmartPLS.

The R^2 value for the dependent variable of Intention to Offend is 0.325, indicating that the variables in the model explained about 33% of the variance in the dependent variable, which, by the standard of structural equation modelling, is moderately high. The R^2 values for the mediating constructs are in the reasonable range of 10%-20%, with the exception of PEB which has a low R^2 of 0.035. This low value suggests that the hypothesized predicator, LSC, cannot explain the variances in PEB alone. Other factors may exist and need further investigation.

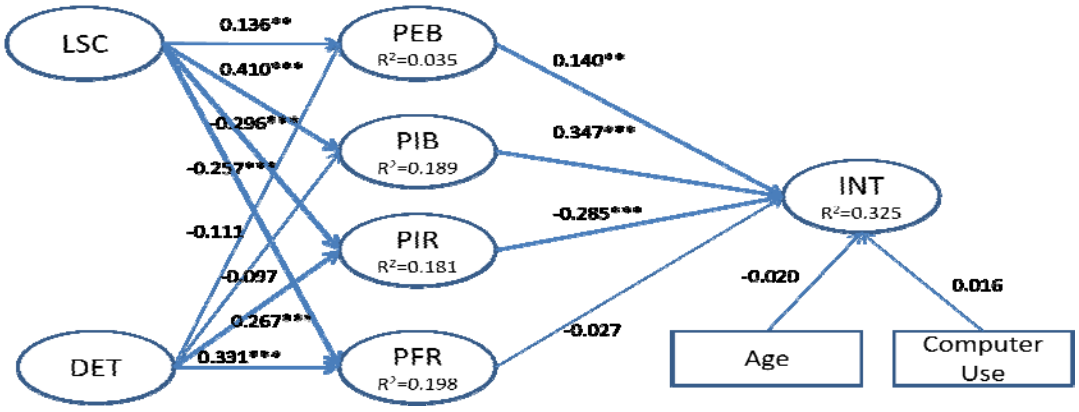

*Figure 2: Results of Structural Analysis (*** 0.01, ** 0.05, *0.1 significant levels)*

The most interesting results from this structural model are about the individual calculus that leads to the intention to commit offences against computer systems in organizational settings. The hypotheses related to the perceived benefits (H1a, β=0.140, $p < 0.05$ and H1b, β=0.346, $p < 0.01$) are supported or strongly supported, while the hypotheses related to the perceived risks H1c (β=-0.284, $p < 0.01$) and H1d (β=-0.028, $p > 0.1$) are mixed. This result reveals that when an individual is contemplating whether to commit offensive behavior toward the organizational computer systems, the perceived benefits dominate the perceived risks in the rational decision making process. The strongly significant path from PIB to INT suggests that the intrinsic satisfaction such as thrill and happiness that would be gained from the offensive act, are even more influential than the extrinsic material gains such as the possession of money and goods, on the behavioral choice of the individual.

Hypothesis	Hypothesized Relationship	Path Coefficient	t-statistic	p-value	Testing Result
H1a	PEB->INT	*0.140*	*2.174*	< 0.05	Supported
H1b	***PIB->INT***	***0.346***	***4.307***	***< 0.01***	***Strongly supported***
H1c	***PIR->INT***	***-0.284***	***3.654***	***< 0.01***	***Strongly supported***
H1d	PFR->INT	*-0.028*	*0.286*	> 0.1	Not supported
H2a	LSC->PEB	*0.136*	*1.743*	< 0.05	Supported
H2b	***LSC->PIB***	***0.410***	***4.779***	***< 0.01***	***Strongly supported***
H2c	***LSC->PIR***	***-0.296***	***3.847***	***< 0.01***	***Strongly supported***
H2d	***LSC->PFR***	***-0.257***	***3.320***	***< 0.01***	***Strongly supported***
H3a	DET->PEB	-0.111	1.602	> 0.1	Not supported
H3b	DET->PIB	-0.097	1.434	> 0.1	Not supported
H3c	***DET->PIR***	***0.267***	***3.884***	***< 0.01***	***Strongly Supported***
H3d	***DET->PFR***	***0.331***	***4.515***	***< 0.01***	***Strongly supported***

Table 5: Latent Variable Correlations

Perhaps even more interesting is the insignificance of the hypotheses related to deterrence. Our data show that deterrence impacts individual intention to commit computer offences primarily through increasing the perceived informal risks by the individual. While deterrence, which is modelled as a second order reflective construct of certainty, severity, and celerity of punishment for computer offences in organizations, significantly impacts the perceived informal risks (H3c, β=0.267, $p<0.01$) and perceived formal risks (H3d, β=0.331, $p < 0.01$), only the perceived informal risks has a significantly negative influences on the individual's intention to commit computer offenses.

Last but not the least, the role of low self-control in explaining deviant behavior has once again been confirmed in the context of computer offence. The causal chain from self-control to offensive behavior is explained by our research model and confirmed by the data. Individuals with low self-control are more likely to be tempted by the appeal of the offensive act in terms of perceived benefits of the act, and thus more likely to commit the act. This is because low self-control leads to higher levels of perceived extrinsic benefits (H2a, β=0.136, $p<0.05$) and perceived intrinsic benefits (H2b, β=0.410, $p<0.01$), and lower levels of perceived informal risks (H2c, β=-0.296, $p<0.01$) and formal risks (H2d, β=-0.257, $p<0.01$), which in turn strongly influence the intention to commit the abusive act (H1a and H1b). These results are summarized in Table 5.

5 DISCUSSION

Our structural equation modelling results using data collected from employees in five Chinese companies have provided strong support to our research model and hypotheses. Out of the 12 hypothesized relationships, seven are strongly supported at the $p<0.01$ level, two are supported at the $p <0.05$ level, and the remaining three are not supported ($p>0.1$). These results have significant theoretical and practical implications for information security research and management. We now discuss some of these implications and potential future research directions.

Our results suggest that computer offences by employees are primarily a result of overestimating the benefits and underestimating the risk by employees when the situations for committing the offences present themselves and the employees have the means to conduct the offensive acts. In their rational analyses about each scenario, perceived benefits seem to dominate perceived costs. This is consistent with the findings of Tunnell (1990) in a criminology study that criminal offenders primarily think about positive consequences and less about negative consequences. Furthermore, Akers (1999, p. 20) pointed out that the threat of sanctions only has limited marginal effect on criminal behavior, as evidenced by the weak link between capital punishment and the rate of homicides. The critical question to both criminology and information security is why it is so. This is certainly an important issue for future research.

On the other hand, our results also suggest what might help lower the perceived benefits and increase the perceived risks of committing offensive acts and thus reduce computer offences in organizations. Our results show that employees with low self-control, those who are more concerned about themselves than others, who are more interesting in what happens now than in the future, and those

who are more risk taking than risk averse, are more likely to overestimate the benefits of offensive acts. In addition, our results show that deterrence can increase the perceived risks and thus reduce the intention to commit computer offences only to a limited degree. These findings imply that both psychological screening of employees and implementing strong security policies and rules can be effective in reducing internal computer crimes and offences. However, given the dominance of the perceived benefits in the offensive calculus, hiring employees with higher level of self-control and assigning them to sensitive positions seem to be more effective than enforcing strict punishments.

6 CONCLUSION

In this study, we developed and tested an integrated model of computer offences by employees in organizational settings based on multiple criminology theories. We found that the rational choice framework of computer offense is largely supported. However, the most interesting finding is that the perceived benefits of offensive acts dominate the perceived risks of the offensive acts in the rational calculus. As a result, the deterrence antecedents may be less effective than the self-control antecedents in the rational decision calculus of an individual.

We must acknowledge that this study has a number of limitations. First and foremost, the research hypotheses are not yet well developed and the majority of the hypotheses are deducted directly from their base theories without substantial evidence from the literature. It is our intention to focus on the presentation of the ideas rather than seeking rigor in hypothesis development in this early stage of the study. Second, the literature review is still incomplete in many aspects. We intend to conduct a comprehensive literature search and review in the next stage of this research and address these limitations in future research.

References

Ajzen, I. (2002) Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. Journal of Applied Social Psychology, 32, 665-683.

Akers, R. (1999) Criminological Theories. Fitzroy Dearborn Publishers, Chicago, IL.

Anderson, J.C., and Gerbing, S.W. (1988) Structural Equation Modeling in Practice: a Review and Recommended Two-Step Approach. Psychological Bulletin, 103(3), 411-423.

Antia, K.D., Bergen, M.E., Dutta, S., and Fisher, R.J. (2006) How Does Enforcement Deter Gray Market Incidence? Journal of Marketing, 70(1), 92-106.

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

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

Becker, G. (1968) Crime and Punishment: An Economic Approach. Journal of Political Economy, 76(2), 169-217.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., and Boss, R. W. (2009) If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. European Journal of Information Systems, 18, 151-164.

Chin, W.W. (1998) The Partial Least Squares Approach to Structural Equation Modeling, in Modern Methods for Business Research, G.A. Marcoulides (ed.), Lawrence Erlbaum Associates, Hillsdale, NJ. 295-336.

Cornish, D. B. and Clarke, R. V. (1986) The Reasoning Criminal: Rational Choice Perspectives on Offending. New York: Springer-Verlag.

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.

Dinev, T. and Hu, Q. (2007) The Centrality of Awareness in the Formation of User Behavioral Intentions towards Preventive Technologies in the Context of Voluntary Use. Journal of the Association for Information Systems, 8(7), 386-408.

Ernst & Young (2008) Global Information Security Survey. Ernst & Young, http://www.ey.com.
Fornell, C. and Larcker, D.F. (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18, 39–50.
Gefen, D., Straub, D.W., Boudreau, M.C. (2000) Structural Equation Modeling and Regression: Guidelines For Research Practice. Communications of AIS, 4, Article 7.
Gettfredson, M. and Hirschi. T. (1990) A General Theory of Crime. Stanford University Press, Stanford, CA.
Gibbs, J. P. (1975) Crime, Punishment, and Deterrence. Elsevier, New York, NY.
Grasmick, H. G., and Bursik, R. (1990) Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model. Law & Society Review. 24, 837-861.
Grasmick, H., Tittle, G., Bursik Jr., R., and Arneklev, B. (1993) Testing the Core Implications of Gettfredson and Hirschi's General Theory of Crime. Journal of Research in Crime and Delinquency, 30, 5-29.
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
Hulland, J. (1999) Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. Strategic Management Journal, 20, 195–204.
Kankanhalli, A., Teo, H.H. ,Tan, B.C.Y., and Wei. K.K. (2003) An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management, 23(2), 139–154.
Nagin, D.S. and Paternoster, R. (1993) Enduring Individual Differences and Rational Choice Theories of Crime. Law & Society Review, 27(3), 467-496.
Paternoster, R and Simpson, S. (1993) A Rational Choice Theory of Corporate Crime, in R. V. Clarke & M. Felson, (eds.) Advances in Crimino logical Theory (v5): Routine Activity and Rational Choice, Transaction Books, New Brunswick, NJ.
Paternoster, R. and Simpson, S. (1996) Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. Law & Society Review, 30(3) 549-583
Paternoster, R., Saltzman, L.E., Waldo, G.P., and Chiricos, T.G. (1983) Perceived Risk and Social Control: Do Sanctions Really Deter? Law & Society Review, 17(3), 457-480
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.
Raykov, T. (1998) Coefficient Alpha and Composite Reliability with Interrelated Nonhomogeneous Items. Applied Psychological Measurement, 22 (4), 375-385
Ringle, C.M., Wende, S., and Will, A. (2005) SmartPLS, 2.0 (beta), University of Hamburg, Hamburg, Germany, available on the Web at http://www.smartpls.de
Straub, D. W. (1990) Effective IS Security: An Empirical Study. Information Systems Research, 1(3), 255–276.
Straub, D.W. and Nance, W.D. (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly, 14(1), 45–60.
Straub, D.W. and Welke, R.J. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22(4), 441-469.
Straub, D.W., Boudreau, M.C., and Gefen, D. (2004) Validation Guidelines for IS Positivist Research. Communications of the AIS, 13, 380-427.
Simpson, S.S., Piquero, N.L., and Paternoster, R. (2002) Rationality and Corporate Offending Decisions, in A. R. Piquero and S. G. Tibbetts (Eds.) Rational Choice and Criminal Behavior – Recent Research and Future Challenges, Routledge, New York, NY. 25-39.
Tittle, C.R. (1980) Sanctions and Social Deviance: The Question of Deterrence. Praeger, New York.
Tunnell, K. (1990) Choosing Crime: Close Your Eyes and Take Your Choices. Justice Quarterly, 7(4), 673-690.
Willison, R. (2006) Understanding the perpetration of employee computer crime in the organisational context. Information and Organization, 16, 304–324.
Willison, R. and Backhouse, J. (2006) Opportunities for computer crime: considering systems risk from a criminological perspective. European Journal of Information Systems, 15, 403–414