경영정보학연구
제12권 제1호
2002년 3월

신뢰성이론을 바탕으로 한 통합 컴퓨터 보안 모형에 관한 연구*

이상근**, 유상진***

An Integrated Computer Security Model Based on the General Trust Theory

Lee, Sang-Gun, Yoo, Sangjin

For the last two decades, there has been much research on computer abuse from the perspective of the general deterrence theory based on objectism, which covers security policy, security awareness programs, and physical security system. The traditional view offered by the general deterrence theory indicates that security policy, security awareness, and security system play a major role in preventing computer abuse. In spite of continuous organizational efforts and investments based on these systematic factors, the incidence of computer abuse in organizations is still rapidly increasing. This paper proposes another perspective -- the social control theory based on subjectism -- in preventing computer abuse. According to the social control theory, organizational trust, which comprises organizational attachment, commitment, involvement and norms, can prevent computer abuse by reducing insider's computer abuse.

The aim of this article is to assess the role of organizational trust come from attachment, commitment, involvement, norms in preventing computer abuse. The results indicate that both organizational trust and deterrent factors are effective in preventing computer abuse.

* The authors thank anonymous reviewers of this journal and AMCIS 2001 for their comment on previous drafts of this paper. We especially thank Dr. Sang M. Lee for his substantive suggestions. We also thank the many respondents from the various organizations who participated in the studies and our families.

** Dept. of Management, University of Nebraska-Lincoln
*** 계명대학교 경영학부 경영정보학과

Ⅰ. Introduction

In this customer-centric world of instant access and continuous connection, E-business initiatives that outpace security are a recipe for disaster. From the organizational perspective, one of the roles of information systems is to prevent computer abuse. Managers indicate that security is high on their to-do list. According to InformationWeek [Breidenbach, 2000], nearly three-quarters of 4,900 survey respondents regard computer security as a top priority. Specially, recent research indicates the primary threat of security abuse actually comes from within the organization's insiders such as employers and managers [Olson and Olson, 2000].

With the rising incidence of computer abuse, organizations are looking for better ways to deter computer abuse. Based on the general deterrence theory (GDT), organizations can reduce computer abuse by implementing anti virus systems, using password protection schemes, severely enforcing computer security policies [Beccaria 1963; Paternoster 1987; Smith and Garton 1989], and creating security awareness in employees by security education [Hoffer and Straub 1989; Straub and Nance 1990; Wood 1991}.

Recently, the frequency and volume of abuse are increasing despite organizations' huge investments in deterrent factor to prevent computer abuse. Academia has begun to pay more attention to the human side of computer abuse [Crockett, 1998; McCollum, 1997; Parker, 1981, and 1998]. However, there has been little attention or previous research from the organizational trust perspective in computer abuse deterrence.

The main objective of this article is to apply an integrated model of computer abuse by combining the general deterrence theory (GDT) and the social control theory (SCT). More specifically, we will incorporate the SCT into the existing GDT-based model and assess the degree to which the integrated model explains computer abuse. The findings from this research are helpful to organizations in the enhancement of their computer security systems.

Ⅱ. Literature Review

The literature based on general deterrence theory, explains security measure implemented by organizations rely on technology alone without considering other factors such as people, and process [Eloff and von Solms, 2000; Dhillon and Backhouse, 2000].

Specially, Eloff and von Sloms [2000] provided a hierarchical framework for security management. Their framework includes two major elements, namely, technology and process. However, they do not include another piece of the security puzzle, the human aspect [Andress and Fonseca, 2000]. Recent joint study by the Computer Security Institute (CSI) and the FBI documents that the most serious losses in companies are committed by unauthorized insider access [Power, 2000]. Dhillon and Backhouse [2000] aptly point out that information security system is a social and organizational issue because systems are used by people. Thus, it is the humans that interact with, and are responsible for systems that have the biggest impact on the security of individual systems and the organization as a whole. In this context, personal traits such as responsibility, integrity, trust and ethicality are deemed critical in securing information assets [Dhillon and Backhouse, 2000].

According to Orlikowski and Robey's research [Orlikowski and Robey, 1991; Orlikowski, 1992], they claim that recent work in social theory departs from prior tradition in proposing that social phenomena can be understand as comprising both subjective and objective elements.

In the view of the previous discussion, we contend that for any security solution to be effective, it should take into account the subjective perspective. Thus, we propose social control theory, developed by Agnew, as an aid in helping to explain organizational insiders' computer abuse. Unlike general deterrence theory based on objective elements, Agnew [1992] presented a social control theory of crime and delinquency that overcomes many of the criticisms leveled at an earlier strain theory in the perspective of subjective elements [Bernard, 1984; Cole, 1975]. Agnew's 1992 theory distinguished social control theory from social strain and social learning theories.

According to Agnew [1992, and 1995], social control theory explains negative relationships between independent variables (i.e., delinquent peer group) and dependent variables (i.e., computer abuse, drug, alcohol). That is, a negative affect creates pressure for corrective action, and may lead insiders to: (1) make use of illegitimate channels of goal achievement, (2) attack or escape from the source of their adversity, and (3) manage their negative affect through the use of illicit computer abuse.

According to the social control theory presented by Hirschi [1969], social control was defined as attachment, commitment and norms [Hirschi 1969; Krohn and Massey, 1980, Krohn, 1995; Sampson and Laub 1992; Shoemaker 1990]. Jensen [1986] also argued that Elliott, Hizinga and Ageton's [1985] measures of social control which gives rise to organizational trust, are biased toward the bond of involvement. To overcome this problem, Agnew [1991] developed the elements of social bonds, which are parental attachment, school attachment, commitment, deviant beliefs, and delinquent peers.

On the basis of social control theory, we propose a new set of measures that index the element of organizational trust, and are represented by four factors; attachment, commitment, involvement, and norms [Agnew 1991, and 1993; Anderson et al. 1999; Costello and Vowell, 1999]. We will discuss these factors in more detail in the research model.

Ⅲ. Research Model

Based on the literature review, we developed hypotheses regarding the relationships between: (1) general deterrent factor and computer abuse using the general deterrence theory (GDT), (2) organizational trust factors and computer abuse using the social control theory (SCT), which asserts that the higher the level of organizational trust, the less likely it is for employees to be involved in computer abuse.

3.1 Exogenous Construct - Deterrent construct

Straub [1990] suggested that the set of deterrents to computer abuse is composed of deterrent certainty, IS security efforts, dissemination of information about penalties, guidelines and pPolicies for acceptable system use. A set of rival explanations included preventive security software, motivational factors affecting abuse and environmental factors affecting abuse, such as the tightness of the security environment and visibility of security. Straub also insisted that among the alternative or rival explanations for low levels of computer abuse are countermeasures known as preventives. Classes of preventives include physical security of facilities as well as security software [Hsaio, et al., 1979]. A well-known form of security software, for example, is password protection.

Security policy, according to Kwok and Longley [1999], includes a definition of information security; a statement of management intention supporting the goals and principles of information security; an explanation of the specific security policies; a standards and compliance requirement; a definition of general and specific responsibilities for all aspects of information security; and an explanation of the process for reporting suspected security incidents. Solms [1999] insisted that corporate IT security policies needed to be drafted, taking the IT security objectives, strategies and other policies into account.

Security awareness is a vital part of organizational information security and it is important that there are formal commitments to this topic, and that such formal commitments are communicated to staff [Siponen, 2000]. Thus, the standards recommendations comprise security in job descriptions, recruitment screenings, confidential agreements, information security education and training, reporting of security incidents, reporting of security weaknesses, reporting of software malfunctions, and disciplinary processes [Kwok and Longley, 1999]. It is reasonable to assume that people will still want to achieve and maintain a feeling of security through security procedures, given that such a need can be pointed out or awakened [Siponen, 2000].

Kwok and Longley [1999] emphasized the physical and environmental security system including physical entry controls, security of data centers and computer rooms, isolated delivery and loading areas, removal of property, equipment sitting and production, power supplier, cable security, equipment maintenance, security of equipment off premises, and secure disposal of equipment.

3.2 Exogenous Constructs - Organizational trust constructs

As earlier mentioned, we defined organizational trust constructs as attachments, commitment, involvement, and norms [Hirshi, 1969; Jensen, 1986; Krohn, 1995; Agnew, 1991, and 1993; Sampson and Laub, 1992; Shoemaker, 1990]. Attachment is defined as the affection and respect that an individual has for others-most notably a parental attachment and a school attachment. For example, how much time have you spent talking, working, or playing with your family; how much have your parents influenced what you've thought and done [Paternoster and Mazerolle, 1994].

Commitment referred to the individual's actual or anticipated investment in conventional society, including the individual's reputation, achievements and aspirations. Involvement means the amount of time spent engaged in conventional activities, which reinforces employees' relationships [Jensen, 1986].

Norms refer to the moral validity of the law and it forms the moral element of the bonds [Matsueda 1982; Reed and Rountree 1994; Reed and Yeager, 1996]. It is usually measured in terms of the respondent's attitude toward one or several delinquent acts, although more general measures are occasionally used (e.g., "to intentionally break any law is wrong" and "we all have a moral duty to abide by the law").

In summary, deterrent construct refers to security policies, security awareness, and security systems, while the organizational trust constructs are closely related to attachments, commitments, involvements, and norms.

3.3 Endogenous construct - computer abuse

The two quantitative items that were used to measure computer abuse are: (1) The frequency of computer abuse within the same industry, and (2) end users' perception of the frequency of computer abuse. These measures were adapted from other computer security sur-

<Table 1> Concepts, Constructs, and Measures of The Research Model

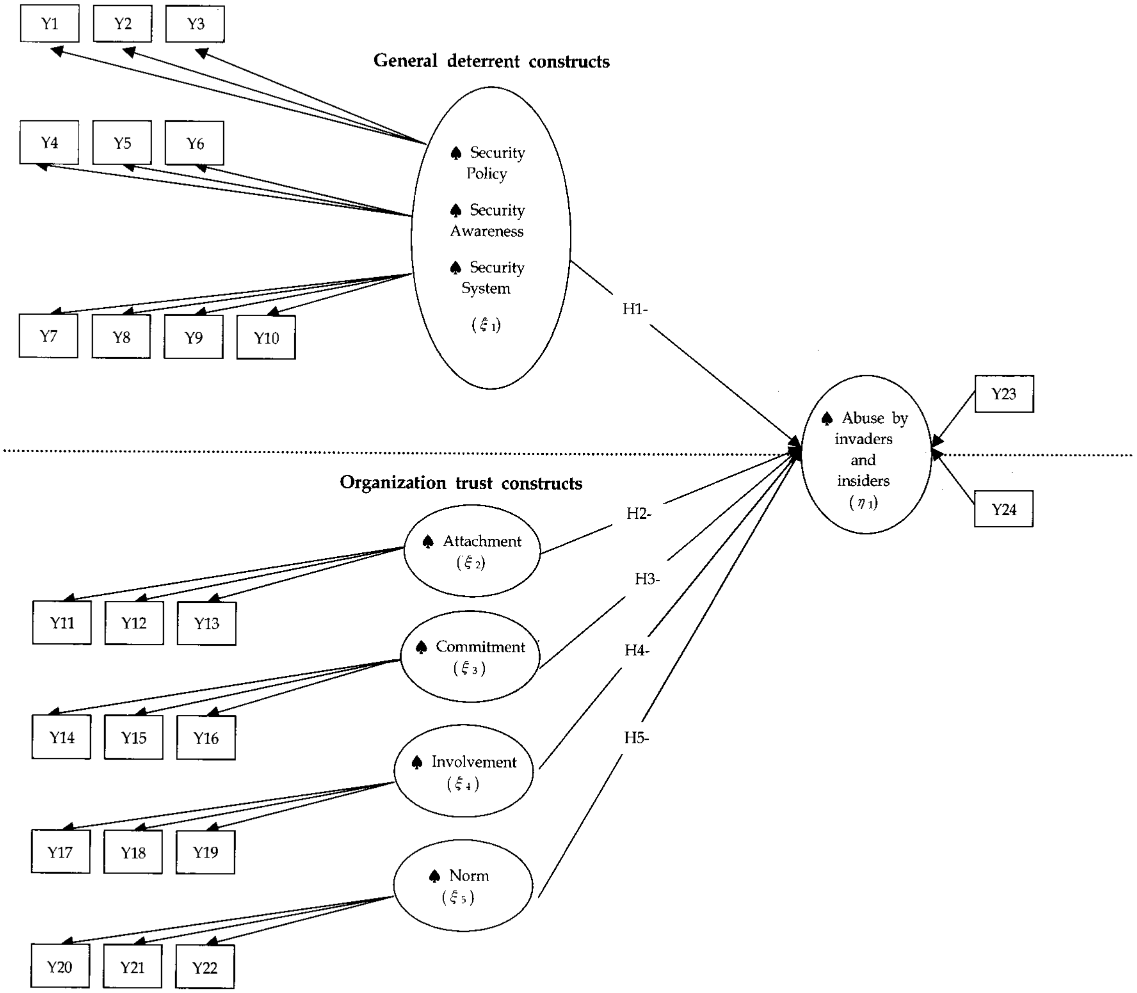
Concepts	*Constructs*	*Measure Description*
General Deterrence Theory	Security policy	• Effectiveness of security policy (Y1) • Severity of security policy (Y2) • Helpfulness of security policy (Y3)
	Security awareness	• Effectiveness of security awareness (Y4) • Severity of security awareness (Y5) • Helpfulness of security awareness (Y6)
	Physical security system	• Degree of security system effectiveness (Y7) • Investment on security system (Y8) • Sufficiency of budget for security system (Y9) • Efficiency of security systems (Y10)
Social Control Theory	Attachment	• Co-workers as being a the very important part of ones business life (Y11) • Respect for Co-worker's views or opinion (Y12) • Reliance on co-workers when they work at your business unit (Y13)
	Commitment	• Desire to succeed within the business unit (Y14) • Enhance your capability to the task (Y15) • Importance for the success of your business unit (Y16)
	Involvement	• Chances to participate in formal meetings (Y17) • Personal relationship with many people (Y18) • Loyalty to the company (Y19)
	Norms	• Moral strength (Y20) • You just do not have any choice but to break the law (Y21) • It is right to get around the law if you can get away with it (Y22)
Computer Abuse	Computer Abuse	• Frequency of computer abuse within to the industry (Y23) • End users' perception of frequency of computer abuse (Y24)

veys [CSI, 1999; Ernst and Young, 2000; Schaub and Biery, 1995] and research by Dinnie [1999], Thompson [1998], and Straub [1990].

All of the constructs shown in the research model will be operationalized using measures from existing studies. <Table 1> shows the measures of deterrent construct, organizational trust constructs, and computer abuse construct used in this research.

Based on the research model, we developed the following hypotheses regarding the relationship between the exogenous constructs and the endogenous construct using the GDT and the SCT. This research investigates the relationships between the exogenous constructs (deterrent construct and organizational trust constructs) and the endogenous construct (computer abuses); a research model is in <Figure 1>.

Based on the research model and the existing literature on GDT and SCT [Kwok and Longley, 1999; Solms, 1999; Straub, 1990; Agnew 1991, 1992, 1993, and 1995; Agnew and White,



<Figure 1> Theoretical Model of Computer Abuse

1992; Paternoster and Mazerolle, 1994; Elis and Simpson, 1995], which suggest that the deterrence and organizational trust factors can reduce computer abuse or crime, we developed the following hypotheses:

H1: Deterrent construct (include policy, awareness, and security system) will have negative and significant additional explanatory power on computer abuse.

H2-5: Organizations with higher organizational trust constructsfactors will experience less computer abuse computer abuse than organizations with lower organizational trust factors.

H2: The Attachment constructfactor will have negative and significant additional explanatory power on computer abuse.

H3: The Commitment constructfactors will have negative and significant additional explanatory power on computer abuse.

H4: The Involvement constructfactor will have negative and significant additional explanatory power on computer abuse.

H5: The Norms constructfactors will have negative and significant additional explanatory power on computer abuse.

Ⅳ. Research Methodology

4.1 Research design

This survey utilizes a 7-point Likert- type scale. To summarize data and develop constructs, this study uses a path analysis, which provides a simultaneous test of model relationship as well as estimates for measurement error in the constructs. LISREL 8.3 is used to conduct such an analysis.

The measurement model was assessed through confirmatory factor analysis, using maximum likelihood estimation on the covariance matrix [Jreskog and Srbom, 1993a, 1993b, and 1993c]. The tested model specified five exogenous constructs. The first construct is deterrent constructs, which was hypothesized that this construct would be indicated by from Y1 Y10. Another exogenous constructs are attachment, commitment, involvement and norms, which included Y11-Y22.

The research scheme in this paper is the causal analysis from the systematic linkages of deterrent construct, organizational trust constructs to computer abuse construct. As noted earlier, precise definitions for deterrent construct is developed from the general deterrent factor and those of organizational trust constructs come from social control theory.

4.2 Samples of research Model

For the purpose of this study, we used surveys of end-users to test the hypotheses. The survey was distributed to 500 computer users during the fall of 2000 to MBA students, who have full time job, of 5 universities located nation-wide in Korea. We tested the hypotheses proposed above with a sample of 117 among the 130 where the return rate is 26%. Thirteen samples are discarded in this analysis because they have missing variables.

In terms of computer proficiency of participants, most participants were proficient: power

-user (11.5%), above-average (65.1%), and average (19.2%). Only 3.1 percents of participants were novice. In the job carrier, the participants were various: manufacturing (8.5%), financing /banking (7.7%), transportation (1.6%), technology (3.1%), insurance (3.9%), retailing (5.4%), communications (25.6%), education (4.7%), government official (15.5%), health care (7.0%), others were 17.1 percents.

In the research questions addressed the computer abuse, participants had experience of computer abuse: unauthorized use of computer service (22.9%), disruption of computer service (20.2%), data loss (58.0%), hardware loss (22.7%), software loss (30.25).

Finally, the survey showed that abusers were motivated by ignorance of proper professional conduct (58.3%), desire for personal gains (15.1%), misguided playfulness, (19.4), revenge of company (3%), unknown cause (25.4%)

4.3 Reliability and Validity of Research Model

To test consistency or stability, we designed two similar questions about computer security system in the front of questionnaire (question 7) and end of questionnaire (question 14). The

<Table 2> Completely Standard Solution in Computer Security

Constructs and Indicator	Lambda	t-value	Squared Multiple Correlation
• Effectiveness of security policy (Y1)	0.82	6.88	0.35
• Severity of security policy (Y2)	1.21	9.76	0.59
• Helpfulness of security policy (Y3)	0.93	8.36	0.47
• Effectiveness of security awareness (Y4)	0.91	8.29	0.47
• Severity of security awareness (Y5)	1.18	11.41	0.73
• Helpfulness of security awareness (Y6)	1.12	10.38	0.64
• Degree of security system effectiveness (Y7)	1.43	13.48	0.88
• Investment on security system (Y8)	1.47	13.10	0.96
• Sufficiency of budget for security system (Y9)	1.25	10.59	0.66
• Efficiency of security systems (Y10)	1.45	12.94	0.84
• Co-workers as being a the very important part of ones business life (Y11)	0.98	8.92	0.56
• Respect for Co-worker's views or opinion (Y12)	0.95	10.30	0.41
• Reliance on co-workers when they work at your business unit (Y13)	0.90	10.31	0.69
• Desire to succeed within the business unit (Y14)	1.21	11.03	0.73
• Enhance your capability to the task (Y15)	0.54	4.88	0.20
• Importance for the success of your business unit (Y16)	1.25	12.26	0.85
• Chances to participate in formal meetings (Y17)	0.99	9.23	0.59
• Personal relationship with many people (Y18)	0.90	9.31	0.59
• Loyalty to the company (Y19)	1.04	9.09	0.57
• Moral strength (Y20)	0.75	5.79	0.32
• You just do not have any choice but to break the law (Y21)	0.69	5.87	0.33
• It is right to get around the law if you can get away with it (Y22)	1.10	8.21	0.62
• Frequency of computer abuse within to the industry (Y23)	1.18	8.85	0.74
• End users perception of frequency of computer abuse (Y24)	1.29	8.57	0.88

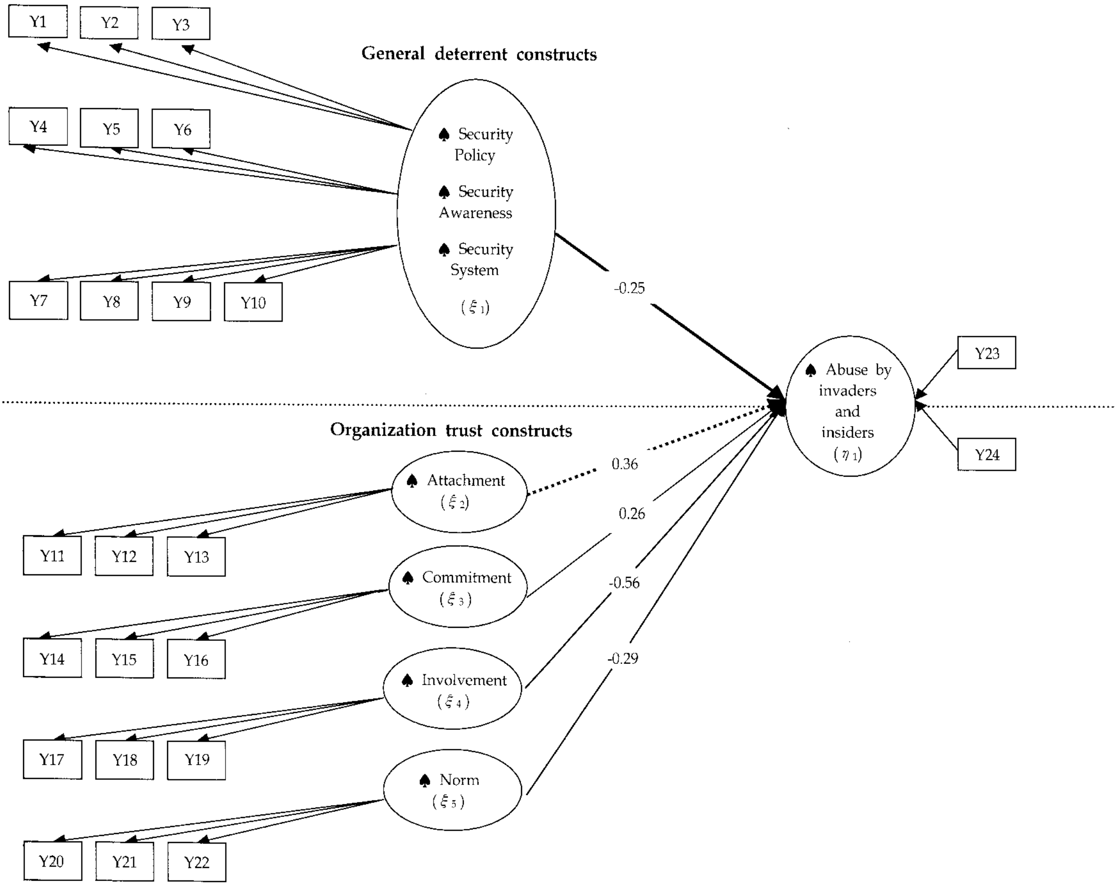
degree of reliability can be represented by a correlation coefficient between the score of two questions [Rosnow and Rosenthal, 1996, p. 136]. The result of Pearson correlation coefficient is 0.606 and is significant at the 99% level.

In the validity of constructs, <Table 2> shows the standardized factor loading (Lambda) and t-values (p<0.05) for the measurement portion of the EQS analysis [Pedhazur, 1997, pp. 821-822]. As is apparent from the tables, most of variables are loaded significantly on the factors on which they are hypothesized to load (Lapierre et al, 1999).

A *p* value greater than 50% implies that the variance captured by trait was more than captured by error components [Bagozzi, 1981]. Finally, the squared multiple correlations of the individual items give an indication of the lower bound of the reliability of the measures. Most of the Squared multiple correlations are above .40, indicating a moderate revel of reliability

V. Results of Lisrel Analysis

<Figure 2> provide a full model that is tested, while <Table 3> presents the standardized path coefficients and the t-values of the model.



<Figure 2> LISREL Path in SEM

Thickbroad lines in the figures indicate the significant paths among latent constructs and thinnarrow line represents no significant paths. As shown in <Figure 2>, and <Table 3>, deterrent factors negatively affects computer abuse. In case of organizational trust factors, involvement and norms have significant level of 0.1. However, contrary to the hypotheses, attachment is positively significant (at 0.1 significant level) in computer abuse.

<Table 3> Results for Hypotheses in Japan

Paths From To	Standardized Paths Coefficient	t-value
Deterrent Factor	-0.25**	-2.10
Attachment	0.36*	1.76
Commitment	0.26	0.99
Involvement	-0.56*	-1.75
Norms	-0.29*	-1.68
Computer abuse		

Note) * : $p<0.10$, ** : $p<0.05$

The measures of overall goodness-of-fit for the entire model are good (see <Table 4>). The calculations are as follow: (remembering Chi-squire/degrees of freedom less than 3 is very good). The value of our model is 2.220. In the NNFI and NFI, the values are 0.84 and 0.78 and in the AGFI and GFI, 0.65 and 0.73, these measures are acceptable [Gefen et al.].

<Table 4> Measures of Model Fitness

Fit measure	Recommended Value	Fitness Measure
Chi-Square		243.46
Chi-Squre/df	<= 3.0	2.220
NNFI	>= 0.90	0.84
AGFI	>= 0.80	0.65
SRMR	<= 1.0	0.12
RMSEA	<= 0.1	0.10

Ⅵ. Findings

<Table 3> summarizes the results from the coefficients of path. The R^2 scores indicate that the 5 constructs constitute good predictors of computer abuse (Multiple R^2=0.270).

The deterrent factor (security policy, security awareness and security system) appears to be the most significant predictor among the constructs (γ_1= -0.250, t= -2.10). As many researchers [Hsaio, et al., 1979; Hoffer and Straub, 1989; Straub, 1990; Straub and Nance 1990; Straub et al, 1997 and 1998; Kwok and Longley, 1999; Solms, 1999 and; Siponen, 2000) have insisted that the deterrent factor to computer abuse is efficient to protect against computer abuse. That is, this empirical test identified that security system efforts including security operating system, access control software and hardware, DBMS security systems, firewall systems, intrusion detection systems, anti-virus systems, digital ID systems, and security policies including oral admonishment, written admonishment, suspension, resignation, firing referral to law enforcement, and out-of-settlement, security awareness including training, poster, newsletter trinkets with a security message are each efficient to protect against computer abuses.

The other findings from the path analysis show that the involvement construct is statistically significant, has a strongly negative coefficient (γ_4=0.56, t=-1.77). In addition, the norm construct is also strong and significant (γ_5=-0.290, t=-1.68). However, the attachment construct has a positive coefficient (γ_2 =0.36, t=1.76), although commitment is positive coefficient, it is not significant (γ_3=0.26, t=-0.99).

According to the social control theory [Agnew 1993, and 1995; Hirschi 1969], we assume that all people have a negative behavior of computer abuse if they participate in official meeting or unofficial meeting with organizational trust. Specially, as many of researchers [Matsueda 1982; Reed and Rountree 1994; Reed and Yeager, 1996] suggested that perception of social norms affects computer abuse, our empirical test also suggests that social norms negatively affect computer abuse. The results showed that our hypotheses are partially accepted.

The contrary to hypotheses, attachment is positive on computer abuses. A plausible explanation is that computer abusers who want to steal or commit other computer-related abuses computer needs more information about victims of computer abuses.

Ⅶ. Conclusion

This study sees that the main contribution of this study is to introduce social control theory into research on computer abuse. Until now, this study believes that most researchers have studied computer abuse using the general deterrence theory in the perspective of objectism. This study is the first use of social control theory in the literature on computer abuse in the perspective of subjectism.

This study empirically investigates the application of general deterrence theory and social control theory in the context of computer abuse. The construct of general deterrence theory includes security policy, security awareness, and security systems. In the social control theory, the constructs are involvement, commitment, attachment, and norm.

This study examines constructs influencing computer abuse. With the exception of the attachment and commitment, the other independent constructs, deterrent construct, involvement and norms constructs, have an impact on computer abuse. The conceptual model draws upon new factors (organizational trust constructs) aimed at preventing computer abuse based on the Social control theory. This theory explains that organizational trust, which generates social bonds, also affects behavior to commit computer abuse, whereas the general deterrence theory explains that security policy, security awareness programs, and system access controls prevent computer abuse.

A new integrated theory, namely General Trust Theory, is developed and validated. It will suggest that the enhancement of social bonds through organizational trust is another effective mechanism that might help prevent computer abuse in organizations

As with all survey-type studies, the interpretation of the results of this study should make allowances for sampling limitations of its methodology. Possible limitation is that the samples selected for this research may not be representatives of all computer end users, while the subjects from 5 MBA students' end users. Another possible limitation is that this study did not distinguish insiders' and invaders' abuses and did not consider end users' specific behavior pattern such as intention [Davis, 1986, and 1989; Davis et al., 1989; Mathieson, 1991].

〈참 고 문 헌〉

[1] Agnew, R., "A Longitudinal Test of Social Control Theory and Delinquency," *Journal of Research in Crime and Delinquency,* Vol. 28, No. 2, May 1991, pp. 126-156.

[2] Agnew, R., "Foundation for a Social Control Theory of Crime and Delinquency," *Criminology,* Vol. 30, No.1, 1992, pp. 47-87.

[3] Agnew, R., "Why Do They Do It? An Examination of The Intervening Mechanisms between Social Control Variables and Delinquency," *Journal of Research in Crime and Delinquency,* Vol. 30, No. 3, August 1993, pp. 245-266.

[4] Agnew, R., "Testing The Leading Crime Theories: An Alternative Strategy Focusing on Motivational Process," *Journal of Research in Crime and Delinquency,* Vol. 32, No. 4, November 1995, pp. 363-398.

[5] Agnew, R., and White H.R., "An Empirical Test of Social Control Theory," *Journal of Research in Crime and Delinquency,* Vol. 30, No. 4, 1992, pp. 475-498.

[6] Anderson, B., M.D. Homes, M.D., and Ostresh, E., "Male and Female Delinquent's Attachment and Effects of Attachments on Severity of Self-Reported Delinquency," *Crime Justice and Behavior,* Vol.26, No. 4, Dec. 1999, pp. 435-452.

[7] Andress, M., and Fonseca, B., "Manage People to Protect Data," *InfoWorld.com,* Nov. 2000.

[8] Bagozzi, R, P., "An Examination of the Validity of Two Models of Attitude," *Multivariate Behavioral Research,* Vol. 16, 1992, pp. 323-359.

[9] Beccaria, C., *On Crime and Punishments,* Indianapolis, IN, Bobbs Merril, 1963.

[10] Bernard, T.J., "Control Criticism of Strain Theory: An Assessment of Theoretical and Empirical Adequacy," *Journal of Research in Crime and Delinquency,* Vol. 21, 1984, pp. 353-372.

[11] BreidenbachInformationweek, S., "How Secure Are You?" *Informationweek,* August, 2000, pp. 71-78.

[12] Cole, S., "The Growth of Scientific Knowledge: Theories of Deviance as a Case Study," In *Lewis A. Caser (ed.), The Idea of Social Structure: Papers in Honor of Robert K. Merton,* Harcourt Brace, NY, Javanovich, 1975.

[13] Computer Security Institute, *Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey,* March 1999.

[14] Costello, B.J., and Vowell, P.R., "Testing Control Theory and Differential Association: A Reanalysis of the Richmond Youth Project Data," *Criminology,* Vol. 37, No. 4, 1999, pp. 815-840.

[15] Crockett, J., "Employee Awareness: A Good Bet for Better Security," *Consulting- Specifying Engineer,* 1998, pp. 20-21.

[16] Davis F.D., "A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results," *Doctoral dissertation,* MIT Sloan School of Management, Cambridge, MA, 1986.

[17] Davis F.D., "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly,* Vol. 13, No. 3, September 1989, pp.

319-339.

[18] Davis F.D., Bagozzi, R.P., and Warshaw, P.R., "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science*, Vol. 35, No. 8, August 1989, pp. 982-1003.

[19] Dhillon, G., and Backhouse, J., "Information System Security Management in the New Millenniem," *Communications of ACM*, Vol. 43, No. 7, July 2000, pp. 125-128.

[20] Dinnie, G., "The Second Annual Global Information Security Survey," *Information Management & Computer Security*, Vol.7, No. 3, 1999, pp. 112-120.

[21] Elis L., and Simpson, S.S., "Informal Sanction Threats and Corporate Crime: Additive Versus Multiplicative Models," *Journal of Research in Crime and Delinquency*, Vol. 32, No. 4, Nov. 1995, pp. 399-424.

[22] Eloff, M.M., and von Solms, S.H., "Information Security Management: A Hierarchical Framework for Various for Approaches," *Computer and Security*, Vol. 19, No. 3, 2000, pp. 243-256.

[23] Elliott, D.S., Huizinga, D., and Ageton, S., *Explaining Delinquency and Drug Use*, Beverly Hill, CA, Sage, 1985.

[24] Ernst and Young, *Executive Guide to Internet Security*, Information Systems Assurance and Advisory Services, 2000.

[25] Gefen, D., Straub, D., and Boudreau, M., "Structural Equation Model and Regression: Guideline for Research Practice," *Communication of AIS*, Vol. 4 Article 7, 2000, pp. 1-77.

[26] Hirschi, T., *Causes of Delinquency*, University of California Press, Berkeley, CA, 1969.

[27] Hoffer, J.A., and Straub, D.W., "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Review*, Vol. 30, No. 4, Summer 1989, pp. 35-44.

[28] Hsaio, .K., k., Kerr, D., and Madnick, S., *Computer Security*, Academic Press, New York, 1979.

[29] Jenkins, P.H., "School Delinquency and The School Social Bond," *Journal of Research in Crime and Delinquency*, Vol. 34, No. 3, August 1997, pp. 337-367.

[30] Jensen, G.F., "Dis-Integrated theory: A Critical Analysis of Attempts to Save Strain Theory," *Proceedings of the American Society of Criminology*, Atlanta, GA, 1986.

[31] Jreskog, K.G., and Srbom, D., *New Features in PRELIS 2*, Chicago: Scientific Software, 1993a.

[32] Jreskog, K.G. and Srbom, D., *New Features in PRELIS 8*, Chicago: Scientific Software, 1993b.

[33] Jreskog, K.G., and Srbom, D., *LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language*, Chicago: Scientific Software, 1993c.

[34] Krohn, M., and Massey, J., "Social Control and Delinquent Behavior: An Examination of the Elements of the Social Bonds," *The Sociological Quarter*ly, Vol. 21, 1980, pp. 529-543.

[35] Krohn, M., "Control and Deterrence Theories of Crime," in *Criminology: A contemporary Hand book*, edited by Joseph F. Sheley, Belmont, CA, Wadsworth, 1995, pp. 329-347.

[36] Kwok, L.F., and Longly, D., "Information Security Management and Modeling," *Information Management & Computer Security*,

Vol. 7, No. 1, 1999, pp. 30-39.

[37] Lapierre, J., Filiatrault, P., and Chebet, J., "Value Strategy rather than Quality Strategy: A Case of Business to Business Professional Service," *Journal of Business Research*, Vol. 45, 1999, pp. 235-246.

[38] Mathieson, K., "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior," *Information System Research*, Vol. 2, No. 3, 1991. pp. 173-191.

[39] Matsueda, R.L., "Testing Control Theory and Differential Association: A Casual Modeling Approach," *American Sociological Review*, Vol. 47, 1982, pp. 489-504.

[40] McCollum, T., "Computer Crime," *Nation's Business*, Nov. 1997, pp. 18-26.

[41] Nance, W.D., and Straub, D.W., "An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse," *Proceedings of the 9th International Conference on Information Systems (ICIS)*, Minneapolis, MN, Dec. 1988, pp. 283-294.

[42] Olson, J.S., and Olson, G.M., "I2i trust in e-commerce," *Communications of ACM*, Vol. 43, No. 12, Dec. 2000, p. 41.

[43] Orlikowski, W., and Robey, D., "Information Technology and the Structuring of Organizations," *Information Systems Research*, Vol. 2, No. 2, 1991, pp. 143-169.

[44] Orlikowski, W., "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science*, Vol. 3, No. 3, 1992, pp. 398-427.

[45] Parker, D.B., *Computer Security management*, Reston, VA, 1981.

[46] Parker, D.B., *Fighting Computer Crime - A New Framework for Protecting Information*, John Wiley & Sons, New York, 1998.

[47] Paternoster, R.L., "The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues," *Justice Quarterly*, 1987, pp. 173-217.

[48] Paternoster, R.L., and Mazerolle, P., "The Social control Theory and Delinquency: a Replication and Extension," *Journal of Research in Crime and Delinquency*, Vol. 31, No. 3, August 1994, pp. 235-263.

[49] Pedhazur, E.J., *Multiple Regression in Behavior Research: Explanation and Prediction*, 3rd Edition, Harcourt Brace College Publishers, Fort Worth, TX, 1997.

[50] Power, R., *Tangled Web: table of Digital Crime from the Shadows of Cyberspace*, Que/Manmillan publishing, New York, August 2000.

[51] Reed, G.E., and Rountree, P.W., "Susceptibility to Peer Pressure and Adolescent Alcohol Use," *Proceedings of the American Society of Criminology*, Miami, FL, 1994.

[52] Reed, G.E., and Yeager, P.C., "Organizational Offending and Neoclassical Criminology: Challenging the Reach of a General Theory of Crime," *Criminology*, Vol. 34, 1996, pp. 357-382.

[53] Rosnow, R.L. and Rosenthal, R., *Beginning of Behavioral Research*, 3rd edition, 1996.

[54] Sampson, R.J., and Laub, J.H., *Crime in the Making: Pathways and Turning Points Through Life*, Cambridge, Mass.: Harvard University Press, 1992.

[55] Schaub, J.L., and Biery, K.D., *The Ultimate Computer Security Survey*, Butterworth Heinemann, Newton, MA, 1995.

[56] Shoemaker, J.F., *The Theories of Delinquency*,

Oxford University Press, UK, 1990.

[57] Siponen, M., "A Conceptual Foundation for organizational Information security awareness," *Information Management & Computer Security,* Vol. 8, No. 1, 2000, pp. 31-41.

[58] Smith, D.A., and Garton, P.R., "Specifying Specific Deterrence," *American Sociological Review,* Vol. 54, 1989, pp. 94-106.

[59] Solms, R.V., "Information Security Management: Why Standards are Important," *Information Management & Computer Security,* Vol. 7, No. 1, 1999, pp. 50-57.

[60] Straub, D.W., "Effective IS Security: An Empirical Study," *Information Systems Research,* Vol. 1, No. 3, 1990, pp. 255-276.

[61] Straub, D.W., Keil, M., and Brenner, W., "Testing the Technology Acceptance Model across Cultures: a Three Country Study," *Information & Management,* Vol. 21, No. 1, 1997, pp. 1-11.

[62] Straub, D.W., and Nance, W.D., "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly,* Vol. 14, No. 1, March 1990, pp. 45-62.

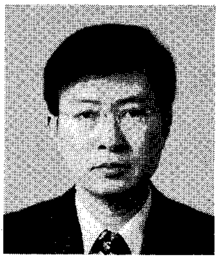
[63] Straub, D.W., and. Welke, R.J., "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly,* Vol. 22, No. 4, Dec. 1998, pp. 441-465.

[64] Thompson, D., "1997 Computer Crime and Security Survey," *Information Management & Computer Security,* Vol. 6, No. 2, 1998, pp. 78-101.

[65] Wood, C.C., *Effective Information Security Management*, Oxford, UK, Elsevier Advanced Technology, 1991.

◆ 저자소개 ◆

이상근 (Lee, Sang-Gun)
서강대학교에서 경영학 전공으로 경영학사와 문학석사 학위를 취득한 후, 일본 와세다 대학교에서 경영학 박사과정을 이수하였으며, 현재는 University of Nebraska-Lincoln에서 MIS전공으로 Ph.D 과정에 재학중이다. 주요 관심분야는 e-Business에서의 공급망관리, e-Business 모형, 컴퓨터 보안 그리고 객체지향시스템 개발 등이다.



유상진 (Yoo, Sangjin)
서강대학교에서 물리학 전공으로 이학사, 경영학 전공으로 경영학사를 취득한 후, University of Nebraska-Lincoln에서 MIS 전공으로 Ph.D를 취득하였다. 미국 Bowling Green State University에서 MIS 담당 조교수로 근무하였으며, 현재는 계명대학교 경영학부 경영정보학과 교수로 근무중이다. 주요 관심분야는 IS/IT를 활용한 경영혁신이며, California Management Review, Long Range Planning, Organizational Dynamics, Information and Management Science, 경영정보학 연구, 경영과학 등의 국내외 학회지에 50여편의 논문을 발표하였다. 한국정보시스템학회장을 역임하였고, 현재는 한국서비스경영학회 부회장, 대구경북ECRC 전문위원, 대구경북 정보화추진단장, 대한상사중재원 중재인으로 활동하고 있다.

◈ 이 논문은 2001년 4월 11일 접수하여 1차 수정을 거쳐 2002년 1월 12일 게재확정되었습니다.