Available online at www.sciencedirect.com
SCIENCE DIRECT®
Information & Management 41 (2004) 707–718
INFORMATION & MANAGEMENT
www.elsevier.com/locate/dsw

An integrative model of computer abuse based on social control and general deterrence theories

Sang M. Lee[a,*], Sang-Gun Lee[a,1], Sangjin Yoo[b,2]

[a]Department of Management, College of Business Administration, University of Nebraska-Lincoln, Lincoln, NE 68588-0491, USA
[b]Department of Management Information System, College of Business Administration, Keimyung University, Daegu, South Korea

Received 7 August 2002; received in revised form 29 March 2003; accepted 7 August 2003

Available online 27 October 2003

Abstract

In spite of continuous organizational efforts and investments, computer abuse shows no sign of decline. According to social control theory (SCT), ''organizational trust'' can help prevent it by enhancing insiders' involvement in computer abuse. The aim of our study was to develop a new integrative model for analyzing computer abuse through assessing the role of Self Defense Intention (SDI) and Induction Control Intention (ICI). The results show that deterrence factors influence SDI and organizational factors significantly affect ICI and ICI decreases insiders' abuse. Interestingly, SDI negatively affects both insiders' and invaders' abuses.

Keywords: Computer abuse; Organizational trust; End user computing; Telecommunications; Social issues

1. Introduction

In this customer-centric world, E-business initiatives that outpace security measures are a recipe for disaster. From an organizational perspective, one of the roles of information systems (IS) is to prevent computer abuse. Managers indicate that security is high on their to-do list.

The Federal Trade Commission (FTC) estimates that consumers' fears resulted in online sales losses of US$ 2.8 billion in 1999 and the value was expected to rise to US$ 18 billion in 2002 [72]. Indeed, the primary threat of a security breach actually comes from within the organization [51]. According to Breidenbach [14], nearly three-quarters of 4900 survey respondents regarded computer security as the top priority. He also stressed the seriousness of insider computer abuse by quoting Schultz: ''Numerically, more attacks come from the outside now, but . . . one insider with the right skills can ruin your company''.

With the rising incidence of computer abuse, organizations are searching for better ways to deter it. Based on general deterrence theory (GDT), organizations can reduce it by implementing anti-virus systems, using password protection schemes, strictly enforcing computer security policies [11,63], and fostering security awareness in employees through special security education [32,71].

Recently, papers have reported that the frequency and volume of abuse are increasing, despite organizations' investments in deterrence factors. Academia has begun to pay more attention to the human side of

* Corresponding author. Tel.: +1-402-472-3915; fax: +1-402-472-5855.
E-mail addresses: slee1@unl.edu (S.M. Lee), sglee@unlserve.unl.edu (S.-G. Lee), yoosj@kmu.ac.kr (S. Yoo).
[1] Tel.: +1-402-438-8548.
[2] Tel.: +82-53-620-2403.

0378-7206/$ – see front matter
doi:10.1016/j.im.2003.08.008

computer abuse [48,52]. However, there has been little interest in the organizational trust perspective to computer abuse.

The main objective of this paper was to develop an integrative model for analyzing computer abuse by combining GDT and social control theory (SCT). More specifically, this study integrated GDT and SCT into the existing theory of planned behavior (TPB) and assessed the degree to which the integrative model explained computer abuse.

2. Review of relevant literature

GDT explains how security measures implemented by organizations rely primarily on technology without considering other factors, such as people and processes. In particular, Eloff and von Sloms [25] provided a hierarchical framework for security management. Their framework included two major elements: technology and processes. However, they did not include another piece of the security puzzle, the human aspect [9]. A recent joint study by the Computer Security Institute (CSI) and FBI documented that the most serious losses in companies were committed by unauthorized insider access [55,56]. Dhillon and Backhouse [21] pointed out that information security was a social and organizational issue, because people use the system. Thus, it is the humans, interacting with and 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 integrity, trust, and ethics are critical in securing information assets.

We contend that for any solution to be effective it should take into account the human perspective. Thus, we propose SCT, developed by Agnew [2], as an aid in helping explain computer abuse by insiders. He presented a general strain theory of crime and delinquency that overcame many of the criticisms leveled at an earlier strain theory [13,16]. This 1992 theory distinguished social strain theory from social control and learning theories.

According to Agnew [4], SCT explains negative relationships between independent variables (e.g., unhappiness within family and delinquent peer group) and dependent variables (e.g., computer abuse, drug, or alcohol); i.e., 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 SCT presented by Hirschi [31], social control was defined as attachment, commitment and norms [59,61]. Jensen [34] also argued that Elliott et al. [24] measures of social control, which give rise to organizational trust, are biased toward the bond of involvement. To overcome this problem, Agnew [1] developed the elements of social bonds, which include parental attachment, school attachment, commitment, deviant beliefs, and delinquent peers.

On the basis of SCT, 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 [3,8,17,28].

We adopted the research framework from the theory of reasoned action (TRA) [7,27] and theory of planned behavior [6]. TRA extended the relationship between humans' attitude and behavior by suggesting that humans develop behavioral intention before a behavior occurs. In other words, TPB proposes that behavioral intention is a mediating construct in the relationship between attitude and behavior. TPB additionally proposes that behavioral intention is driven not only by attitude but also by subjective norms and perceived behavioral control. TPB has been employed to predict various types of behaviors.

3. Research model

Based on the literature review, we developed a set of hypotheses regarding the relationships between: (1) general deterrence factors and computer abuse through SDI based on GDT, which (SDI) reduces insiders' and invaders' abuse; (2) organizational trust factors and computer abuse through ICI based on the SCT, which imply that the higher the level of organizational trust, the less likely it is for insiders to be involved in computer abuse.

3.1. Exogenous constructs—deterrence factors

Straub and Nance [66] suggested that the set of deterrence related to computer abuse is composed of

deterrent certainty, IS security efforts, and dissemination of information about penalties, guidelines and policies for the acceptable system use. A set of rival explanations included preventive security software, and motivational and environmental factors affecting abuse, such as the tightness of the security environment and visibility of security. Straub [64] also insisted that the alternative or rival explanations for low levels of computer abuse are countermeasures known as preventives. Classes of preventives included the physical security of facilities as well as security software [33]. A well-known form of security software, for example, is password protection.

Security policy, according to Kwok and Longley [41], includes a definition of information security, statement of management intention supporting the goals and principles of information security, explanation of the specific security policies, standards and compliance requirement, definition of general and specific responsibilities for all aspects of information security, and an explanation of the process for reporting suspected security incidents. von Solms [70] argued that corporate IS security policies needed to be drafted, taking the IS security objectives, strategies, and other policies into account.

Security awareness is a vital part of organizational information security, and it is important to have formal commitment to this topic, and such formal commitment must be clearly communicated to staff [62]. The standard recommendations in security awareness are security in job descriptions, recruitment screenings, confidential agreements, information security education and training, reporting of security incidents, security weaknesses, software malfunctions, and disciplinary processes [40]. 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.

Kwok and Longley also emphasized the physical and environmental security systems including physical entry controls, security of data centers and computer rooms, isolated delivery and loading areas, cable security, equipment maintenance, security of equipment off premises, and secure disposal of equipment. von Solms posited that carefully managed products and systems provide a more secure computing base, but nothing can provide a full proof.

3.2. Exogenous constructs—organizational trust

We defined the organizational trust construct in terms of attachment, commitment, involvement, and norms. *Attachment* is the affection and respect that an individual has for others—most notably parental and school attachments. This is shown by the time one spends talking, working, or socializing with family members; how much one's parents influenced what the person has thought and done, etc. [53]. *Commitment* refers to the individual's actual or anticipated investment in conventional society, including reputation, achievements, and aspirations. *Involvement* means the amount of time spent engaged in conventional activities that reinforced employee relationships. *Norms* refer to the moral validity of the law that formed the moral elements of the bond [47,57]. This 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., ''we all have a moral duty to abide by the law'').

In sum, the deterrence constructs refer to security policies, security awareness, and security systems, while the organizational trust constructs are closely related to attachments, commitment, involvement, and norms.

3.3. Endogenous constructs—intentions

This study adopts theory of planned behavior. It has been employed to predict various types of behaviors. We suggested two intentions related to computer abuse: self defense and induction control.

Self Defense Intention (SDI) is the intention to install access control software and intrusion protection software, while *Induction Control Intention* (ICI) is the intent to control another person's identification without authorization and illegally use software that can be accessed only by authorization.

3.4. Dependent construct—computer abuse

The two quantitative items used to measure computer abuse were: (1) the frequency of computer abuse by insiders, including employees and managers, such as data loss, hardware loss, unauthorized ID use, and illegal software copying and (2) the frequency of

Table 1
Concepts, constructs, and measures of the research model

Concept	Construct		Measure description
General deterrence theory	Security policy	Y1	Degree of knowledge of security policy
		Y2	Severity of security policy
		Y3	Helpfulness of security
	Security awareness	Y4	Frequency of awareness programs per year
		Y5	Degree of security awareness
		Y6	Helpfulness of security awareness
	Physical security system	Y7	Degree of security system effectiveness
		Y8	Investment on security system
		Y9	Sufficiency of budget for security system
Social control theory	Attachment	Y10	Conversation with co-workers who are in close relationships
		Y11	Communication with co-workers in my task
		Y12	Respect for co-workers' views or opinions
	Commitment	Y13	Desire to succeed within the business unit
		Y14	Importance for the success of your business unit
		Y15	Spending time or investing time to succeed in the business unit
	Involvement	Y16	Chances to participate in informal meetings
		Y17	Personal relationships with many people
		Y18	Loyalty to the company
	Norms	Y19	No matter how small the crime, breaking the law is a serious matter
		Y20	It is wrong when I break the law
		Y21	It is right to get around the law if I can get away with it
Intention to abuse	Self defense	Y22	Intention to install access control software
		Y23	Intention to install intrusion protection software
	Induction control	Y24	Intention to use another person's ID without authorization
		Y25	Intention to illegally use software that can be accessed by authorization
Computer abuse	Invaders' abuse	Y26	The frequency of computer abuse by invaders such as infection of virus via email or hacking.
	Insiders' abuse	Y27	The frequency of computer abuse by insiders such as data loss, hardware loss, unauthorized ID use and illegal copying of software, and so on.

computer abuse by invaders such as infection of a virus via email and hacking. These measures were adapted from other computer security surveys [26,35,60] and research by Dinnie [22], Thompson [68], and Nance and Straub [50]. All of the constructs were operationalized using measures from previous studies. Table 1 shows the measures of organizational trust factors, deterrence factors, SDI, ICI, and computer abuse used.

Fig. 1 presents the research model. We investigated the relationships between deterrence factors and organizational trust factors, intentions to abuse, and computer abuse.

Previous studies [5,23,45,54,65,67] found that each of the factors has either an independent or a combined effect on the reduction of computer abuse. However, the empirical results have been far from clear. Thus, our study adopted TPB to test the following hypotheses:

H1-3. Organizations with strong deterrence factors in place will show higher SDI regarding computer abuse than those with weak deterrence factors.

H1. A strong security policy factor will have a positive and significant additional explanatory power of SDI related to computer abuse.

H2. An effective security awareness factor will have a positive and significant additional explanatory power of SDI related to computer abuse.

H3. An effective security system factor will have a positive and significant additional explanatory power of SDI related to computer abuse.

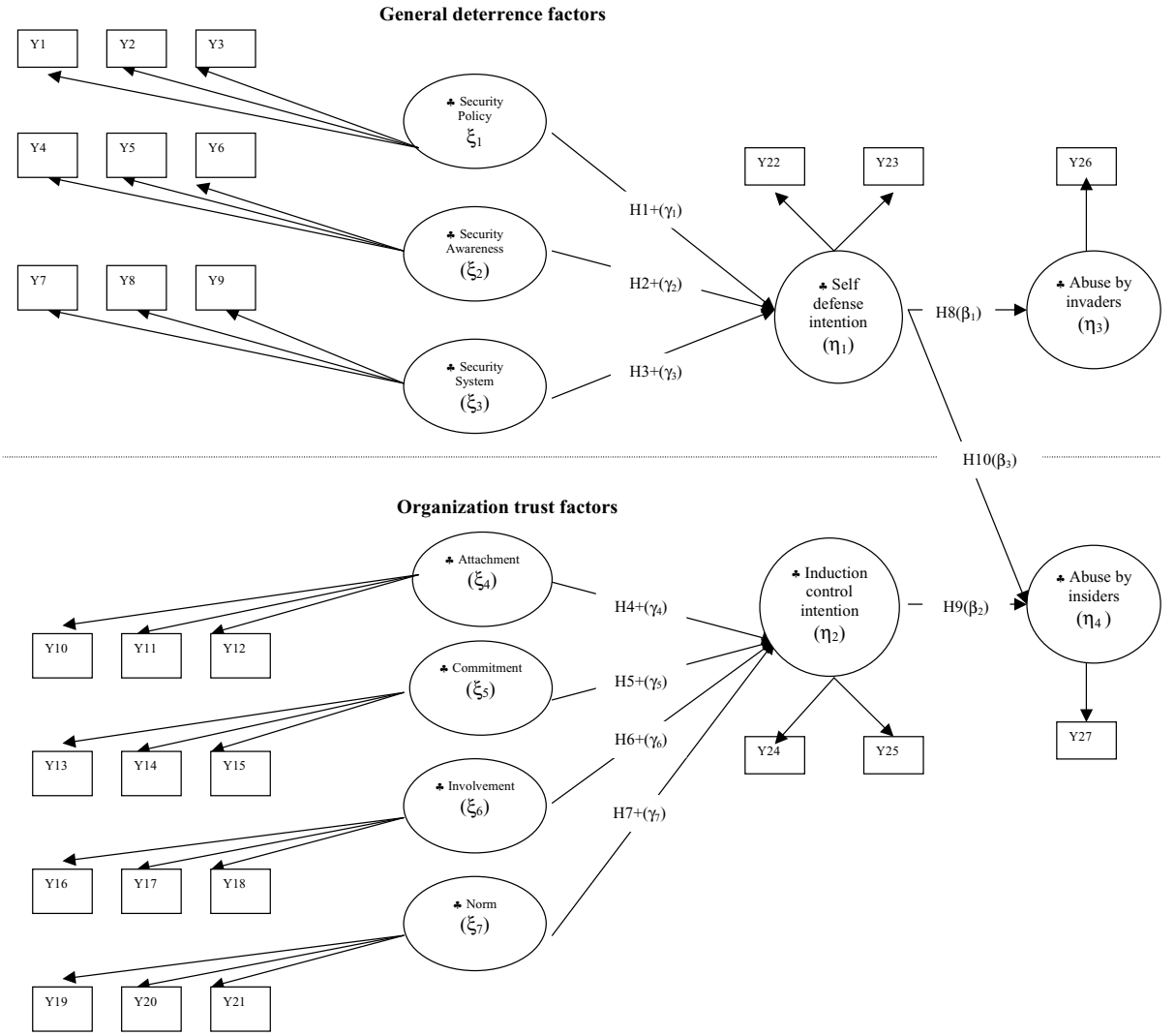

Fig. 1. Theoretical model of computer abuse.

H4-7. Organizations with a higher level of organizational trust will show greater ICI related to computer abuse than those with lower organizational trust.

H4. A higher level of attachment factor will increase ICI related to computer abuse.

H5. A higher level of commitment factor will increase ICI related to computer abuse.

H6. A higher level of involvement factor will increase ICI related to computer abuse.

H7. A higher level of norms factor will increase ICI related to computer abuse.

H8-10. Intentions of self defense and control related to computer abuse will decrease computer abuse.

H8. A higher level of SDI related to computer abuse will decrease invaders' computer abuse.

H9. A higher level of SDI related to computer abuse will decrease insiders' computer abuse.

H10. A higher level of ICI related to computer abuse will decrease insiders' computer abuse.

4. Research methodology

4.1. Sampling procedure

This study utilized a 7-point Likert-type scale for measuring variables. To summarize data and develop constructs, we used the path analysis approach. Maximum likelihood estimation [36–39] was used in the measurement and structural models. This analysis provided a simultaneous test of the model relationships as well as estimates for measurement error.

For the pilot study, the survey questionnaires were distributed to 500 computer users who were MBA students, most with full time jobs, at five universities all located in Korea [43,44]. We performed a pilot test with a sample of 117 from the 130 respondents, a return rate of 26%. In the pilot test, we did not distinguish insiders' and invaders' abuses and did not consider end users' specific behavior patterns, such as intention [18–20,46].

On the basis of the pilot study results, we developed a new questionnaire. The questionnaires were redistributed to the same 500 MBA students and 500 middle managers in six companies (three IT firms, one manufacturer of musical instruments, one department store, and one hospital) in Korea. We then tested the hypotheses with a sample of 182 respondents, a return rate of 18.2%. Among the returned questionnaires, 20 were discarded because of missing items.

Table 2
Characteristics of the sample

Computer proficiency	Proficiency	Frequency	Percentage
	Power-users	22	12.1
	Above-average	49	26.9
	Average	61	33.5
	Below- average	23	12.6
	Novice	16	8.8
	Missing	11	6.0
	Total	182	100.0
Types of industry	Type	Frequency	Percentage
	Transportation	50	27.5
	Manufacturing	34	18.7
	Communications	34	18.7
	Information technology	26	14.3
	Education	10	5.5
	Health care	9	4.9
	Retailing	5	2.7
	Financing/banking	2	1.1
	Missing	12	6.6
	Total	182	100.0
Cause of computer abuse	Type	Frequency (Multiple checking)	Percentage
	Ignorance of proper professional conduct	81	38.57
	Misguided playfulness	52	24.76
	Desire for personal gains	34	16.19
	Unknown reasons	33	15.71
	Revenge on company	4	1.91
	Other	6	2.86
	Total	210	100.00

4.2. Description of the sample

Table 2 presents some characteristics of the sample. In terms of computer proficiency, self rated by the participants, most were proficient: power-users (12.1%), above-average (26.9%), average (33.5%) and below-average (12.6%), novice (8.8%) and no response (6.0%). The participants' jobs were in various industry groups: information technology (27.5%), manufacturing (18.7%), MBA student (18.7%), retailing (14.3%), health care (5.5%), communications (2.7%), financing/banking (1.1%), and no response (6.6%).

Finally, the survey showed that abusers were motivated by ignorance of proper professional conduct (38.57%), misguided playfulness (24.76%), desire for personal gains (16.19%), revenge on the company (1.91%), unknown reasons (15.71%), and other (2.86%).

4.3. Reliability and validity of the research model

To test consistency or stability, we designed two similar questions about computer security systems at the beginning and end of the questionnaire. The degree of reliability can be represented by a correlation coefficient between the scores of two questions [58]. The Pearson correlation coefficient was 0.655 and it was significant at the 0.001 level.

Regarding the convergent validity, Table 3 shows the standardized factor loading (Lambda) and *t*-values ($P < 0.05$) for the measurement portion of the LISREL analysis. As is apparent from table, most variables loaded significantly to their hypothesized factors [42]. A *P*-value greater than 50% implied that the variance captured by trait was more than that captured by error components [10]. Finally, the squared multiple correlation coefficients of individual items give an indication of the lower bound of the reliability of the measures. Most of the squared multiple correlation coefficients were above 40, indicating a moderate level of reliability.

Table 3
Standardized loadings in LISREL analysis

Variables	Lambda	*t*-value[a]	Squared multiple correlation
Y1	0.95	9.12	0.43
Y2	1.16	13.98	0.79
Y3	1.15	12.62	0.69
Y4	1.08	11.98	0.66
Y5	1.09	12.05	0.66
Y6	0.96	9.60	0.47
Y7	1.16	14.25	0.77
Y8	1.16	15.54	0.86
Y9	1.16	13.89	0.74
Y10	1.11	12.75	0.70
Y11	1.13	13.65	0.76
Y12	0.86	11.35	0.59
Y13	1.29	15.16	0.84
Y14	1.27	15.01	0.83
Y15	1.01	11.88	0.61
Y16	1.04	10.65	0.56
Y17	1.03	11.35	0.61
Y18	1.00	10.81	0.57
Y19	1.34	14.57	0.81
Y20	1.50	15.27	0.86
Y21	1.22	11.63	0.59
Y21	1.54	12.21	0.77
Y23	1.70	12.59	0.87
Y24	2.04	12.09	0.79
Y25	2.09	12.23	0.90

[a] $P < 0.001$.

5. Results of LISREL analysis

Fig. 2 provides the full model that was tested, while Table 4 presents the standardized path coefficients and *t*-values of the model. Bold lines in figure indicate the significant paths among latent constructs, thin lines represent non-significant paths and the dotted lines show significant paths rejecting the hypotheses.

The measures of overall goodness-of-fit for the entire model are illustrated in Table 5. The computation procedures were: Using LISREL 8.52, the fitness of the research model was assessed in the results; $\chi^2 = 485.61$ ($P = 0.000$), degree of freedom = 295, χ^2/d.f. = 1.6461, GFI = 0.82, AGFI = 0.77, NFI = 0.83, NNFI = 0.90 and RMSEA = 0.063.

When a model is correct but its conditions may be incorrect, the χ^2-value is likely to appear larger than it should, indicating a problem of fit: the greater the sample size, the lower the χ^2-value. From this perspective, it is therefore advisable to use the χ^2-value in conjunction with other fitness indices. Medsker et al.

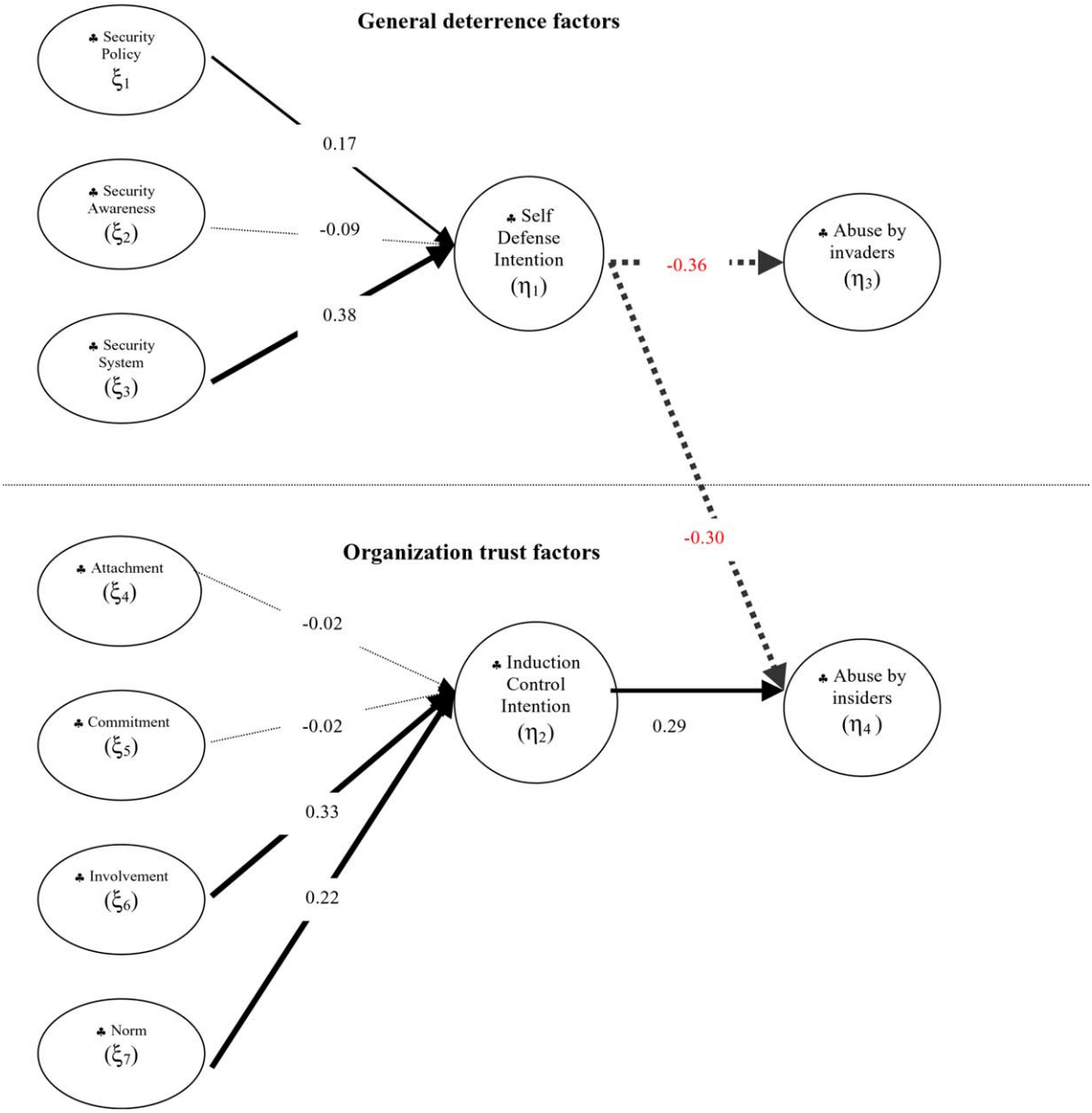

Fig. 2. The results of path analysis.

[49] suggested that χ^2/d.f. ratios of less than 5 can be interpreted as indicating a good fit, with ratios less than 2 indicating over fitting. The current model is reasonable in χ^2/d.f.

The root mean square of approximation (RMSEA) is used to provide guidance on the number of optimal sub-constructs to use. Browne and Cudeck [15] suggest that this index should be lower than 0.08 for a good fit and less than 0.05 for an excellent fit. According to Bentler [12], the value of the normed fit index (NFI) indicates the proportion in the improvement of overall fit of the researcher's model relative to a null

Table 4
Results of hypotheses testing

Paths		R^2	Standardized paths coefficient	Hypotheses
From	To			
Security policy	Self Defense Intention (SDI)	0.20	0.17	Rejected
Awareness			−0.09	Rejected
Security system			0.38***	Accepted
Attachment	Induction Control Intention (ICI)	0.19	−0.02	Rejected
Commitment			−0.02	Rejected
Involvement			0.33**	Accepted
Norms			0.22***	Accepted
SDI	Inside abuse	0.16	−0.30***	Rejected
ICI	Inside abuse		0.29***	Accepted
SDI	Invade abuse	0.13	−0.36***	Rejected

** $P < 0.05$.
*** $P < 0.001$.

Table 5
Measures of model fitness

Fit measure	Recommended value	Fitness measure
χ^2		485.61
χ^2/d.f.	≤3.0	1.1646
NFI	≥0.80	0.83
NNFI	≥0.90	0.90
GFI	≥0.90	0.82
AGFI	≥0.80	0.77
SRMR	≤1.0	0.075
RMSEA	≤0.08	0.063

model. The typical null model is an independence model, that is, one in which the observed variables are assumed to be uncorrelated and their counterpart (non-normed fit index, NNFI) should also have a comparably high value. The values of NFI 0.83 means that the relative overall fit of the model is 83% better than that of the null model estimated with the same data.

The fitness of the overall model was assumed appropriate, based on high fitness indexes, even though the goodness of the fit index (GFI) and adjusted GFI (AGFI) did not satisfy Gefen et al.'s recommended minimum values of 0.90 and 0.80, respectively [29].

6. Findings

Table 4 summarizes the path coefficients for hypotheses testing. The R^2 scores indicated that constructs constituted reasonable predictors of intentions and computer abuse. Fig. 2 presents schematic path analysis.

Among the factors of security policy, security awareness and security system, the security system factor appeared to be the most significant predictor of Self Defense Intention ($\gamma_3 = 0.38, t = 3.11$). Even though the security policy factor was not significant, it also positively affected Self Defense Intention (η_1).

Interestingly, however, the results indicate that the greater the level of Self Defense Intention, the higher the rate of insider and invader abuse. Many researchers have insisted that the deterrence factors related to computer abuse are efficient protection against computer abuse. That is, our empirical test indicated that organizational security system factors including security of the operating system, access control software and hardware, DBMS security systems, firewall systems, intrusion detection systems, anti-virus systems, and digital ID systems were efficient for improving Self Defense Intention. However, it had significantly negative effect on insider and invader abuses. Thus, if computer users had higher SDI, they tended to commit more computer abuse. A possible explanation is that computer abusers who want to steal or commit other computer-related abuses possessed better skills and that computer users who had higher SDI may have tacit and explicit knowledge of computer abuse, such as data loss, hacking, or viruses, so

that they could better recognize their own computer abuses than computer users possessing lower SDI.

On the other hand, SDI may be affected by the results of insider (η_4) or invader abuses (η_3). That is, a computer user may have a higher level of SDI if he/she has experienced being attacked by other abusers. Actually, SDI results from structural aspects of the organization, such as policy, training, and systems. According to structuation theory [30], a recursive relationship between action and structure is grounded in the ongoing practical activities of human agents in particular historical, cultural, and institutional contexts.

Other findings from the path analysis show that the involvement and norms constructs were statistically significant, and had strongly positive coefficients ($\gamma_6 = 0.33$, $t = 2.04$; $\gamma_7 = 0.22$, $t = 2.52$) related to Induction Control Intention (η_2). In addition, the ICI construct was also strong and significant ($\beta_2 = 0.290$, $t = 3.14$) relating to insiders' abuse (η_4). However, the attachment and commitment constructs were not significant ($\gamma_4 = -0.02$, $t = -0.16$; $\gamma_5 = 0.016$, $t = -0.14$).

As social control theory suggests, the results of this study indicated that people tend to have a higher level of ICI if they participated frequently in official or unofficial meetings, had personal relationships with many people, and were loyal to the company. Specifically, Triandis [69] suggested that the perception of social norms strongly affected the prevention of crime. Finally, our empirical test also suggested that ICI affected insiders' computer abuse as the theory of planned behavior assumed.

7. Conclusion

The main reason for this study was to introduce social control theory into research on computer abuse; most prior work had studied computer abuse using general deterrence theory. We empirically investigated the application of general deterrence and social control theories in the context of the theory of planned behavior. The conceptual model drew on the introduction of new factors (attachment, commitment, involvement, and norms) aimed at preventing insider computer abuse based on social control theory.

A new integrative model, general trust theory, was partially developed and validated. It suggested that the enhancement of social bonds through organizational trust was another mechanism that could help prevent computer abuse in organizations.

As with all survey-type studies, the interpretation of the results should make allowances for sampling limitations. One limitation is that the sample, MBA computer users and end users of six companies in Korea, may not be representative of all computer end users. Another possible limitation is that the study might not have included all factors necessary to assess computer use and abuse, including cultural, environmental, or organizational characteristics.

References

[1] R. Agnew, A longitudinal test of social control theory and delinquency, Journal of Research in Crime and Delinquency 28 (2), 1991, pp. 126–156.
[2] R. Agnew, Foundation for a general strain theory of crime and delinquency, Criminology 30 (1), 1992, pp. 47–87.
[3] R. Agnew, Why do they do it?: an examination of the intervening mechanisms between social control variables and delinquency, Journal of Research in Crime and Delinquency 30 (3), 1993, pp. 245–266.
[4] R. Agnew, Testing the leading crime theories: an alternative strategy focusing on motivational processes, Journal of Research in Crime and Delinquency 32 (4), 1995, pp. 363–398.
[5] R. Agnew, H.R. White, An empirical test of general strain theory, Journal of Research in Crime and Delinquency 30 (4), 1992, pp. 475–498.
[6] I. Ajzen, The theory of planned behavior, Organizational Behavior and Human Decision Processes 50, 1991, pp. 179–211.
[7] I. Ajzen, M. Fishbein, Understanding Attitudes and Predicting Social Behavior, Prentice-Hall, Englewood Cliffs, NJ, 1980.
[8] B. Anderson, M.D. Homes, E. Ostresh, Male and female delinquent's attachment and effects of attachments on severity of self-reported delinquency, Crime Justice and Behavior 26 (4), 1999, pp. 435–452.
[9] M. Andress, B. Fonseca, Manage people to protect data, InfoWorld.com, November 2000.
[10] R.P. Bagozzi, An examination of the validity of two models of attitude, Multivariate Behavioral Research 16, 1992, pp. 323–359.
[11] C. Beccaria, On Crime and Punishments, Bobbs Merril, Indianapolis, IN, 1963.
[12] P.M. Bentler, Comparative fit indexes in structural models, Psychological Bulletin 58, 65–79.
[13] T.J. Bernard, Control criticism of train theory: an assessment of theoretical and empirical adequacy, Journal of Research in Crime and Delinquency 21, 1984, pp. 353–372.
[14] S. Breidenbach, How Secure are You?, Information Week, August 2000, pp. 71–78.

[15] M.W. Browne, R. Cudeck, Alternative ways of assessing model fit, Sociological Methods and Research 21, 1992, pp. 230–258.
[16] S. Cole, The growth of scientific knowledge: theories of deviance as a case study, in A. Lewis Caser (Ed.), The Idea of Social Structure: Papers in Honor of Robert K. Merton, Javanovich, Harcourt Brace, NY, 1975.
[17] B.J. Costello, P.R. Vowell, Testing control theory and differential association: a reanalysis of the Richmond youth project data, Criminology 37 (4), 1999, pp. 815–840.
[18] F. D. Davis, 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.
[19] F.D. Davis, Perceived usefulness, perceived ease of use and user acceptance of information technology, MIS Quarterly 13 (3), 1989, pp. 319–339.
[20] F.D. Davis, R.P. Bagozzi, P.R. Warshaw, User acceptance of computer technology: a comparison of two theoretical models, Management Science 35 (8), 1989, pp. 982–1003.
[21] G. Dhillon, J. Backhouse, Information system security management in the new millennium, Communications of the ACM 43 (7), 2000, pp. 125–128.
[22] G. Dinnie, The second annual global information security survey, Information Management & Computer Security 7 (3), 1999, pp. 112–120.
[23] L. Elis, S.S. Simpson, Informal sanction threats and corporate crime: additive versus multiplicative models, Journal of Research in Crime and Delinquency 32 (4), 1995, pp. 399–424.
[24] D.S. Elliott, D. Huizinga, S. Ageton, Explaining Delinquency and Drug Use, Sage, Beverly Hill, CA, 1985.
[25] M.M. Eloff, S.H. von Solms, Information security management: a hierarchical framework for various approaches, Computer and Security 19 (3), 2000, pp. 243–256.
[26] Ernst and Young, Executive guide to Internet security, Information Systems Assurance and Advisory Services, 2000.
[27] M. Fishbein, I. Ajzen, Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research, Addison–Wesley, Reading, MA, 1975.
[28] J. Frank, B. Shamir, W. Briggs, Security-related behavior of PC users in organizations, Information and Management 21 (3), 1991, pp. 127–135.
[29] D. Gefen, D. Straub, M. Boudreau, Structural equation modeling and regression: guidelines for research practice, Communications of the Association for Information Systems 4 (7), 2000, pp. 1–78.
[30] A. Giddens, The Constitution of Society, Bell and Bain Limited, Glasgow, UK, 1984.
[31] T. Hirschi, Causes of Delinquency, University of California Press, Berkeley, CA, 1969.
[32] J.A. Hoffer, D.W. Straub, The 9 to 5 underground: are you policing computer crimes? Sloan Management Review 30 (4), 1989, pp. 35–44.
[33] K. Hsaio, D. Kerr, S. Madnick, Computer Security, Academic Press, New York, 1979.
[34] G. F. Jensen, Dis-integrated theory: a critical analysis of attempts to save strain theory, in: Proceedings of the American Society of Criminology, Atlanta, GA, 1986.
[35] G.W. Joseph, J.E. Blanton, Computer infectors: Prevention, detection, and recovery, Information and Management 23 (4), 1991, pp. 205–216.
[36] K.G. Jöreskog, D. Sörbom, Models search with TERRAD II and RISREL, Sociological Methods and Research 19, 1990, pp. 201–210.
[37] K.G. Jöreskog, D. Sörbom, New Features in PRELIS 2, Scientific Software, Chicago, IL, 1993.
[38] K.G. Jöreskog, D. Sörbom, New Features in PRELIS 8, Scientific Software, Chicago, IL, 1993.
[39] K.G. Jöreskog, D. Sörbom, LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language, Scientific Software, Chicago, IL, 1993.
[40] M.D. Krohn, J.L. Massey, Social control and delinquency: an examination of the elements of the social bond, Sociological Quarterly 21, 1980, pp. 529–543.
[41] L.F. Kwok, D. Longley, Information security management and modeling, Information Management & Computer Security 7 (1), 1999, pp. 30–39.
[42] J. Lapierre, P. Filiatrault, J. Chebet, Value strategy rather than quality strategy: a case of business to business professional service, Journal of Business Research 45, 1999, pp. 235–246.
[43] S. Lee, F. Nah, S. Yoo, An integrated model on computer abuse: a pilot study, in: Proceedings of the 7th Americas Conference on Information Systems, Boston, MA, 2001, pp. 2195–2197.
[44] S. Lee, S. Yoo, The integrated computer security model based on the general trust theory, Journal of Management Information System Review 12 (1), 2002, pp. 123–138.
[45] T. Makkai, J. Braithwaite, The dialectics of corporate deterrence, Journal of Research in Crime and Delinquency 31 (4), 1994, pp. 347–373.
[46] K. Mathieson, Predicting User Intentions: Comparing the technology acceptance model with the theory of planned behavior, Information System Research 2 (3), 1991, pp. 173–191.
[47] R.L. Matsueda, Testing control theory and differential association: a casual modeling approach, American Sociological Review 47, 1982, pp. 489–504.
[48] T. McCollum, Computer crime, Nation's Business, November 1997, pp. 18–26.
[49] G.J. Medsker, L.J. Williams, P.J. Holahan, A review of current practices for evaluating causal models in organizational behavior and human resources management research, Journal of Management 20, 1994, pp. 439–464.
[50] W.D. Nance, D.W. Straub, An investigation into the use and usefulness of security software in detecting computer abuse, in: Proceedings of the 9th International Conference on Information Systems (ICIS), Minneapolis, MN, 1988, pp. 283–294.
[51] J.S. Olson, G.M. Olson, I2i trust in e-commerce, Communications of the ACM 43 (12), 2000, pp. 41–44.
[52] D.B. Parker, Fighting Computer Crime—A New Framework for Protecting Information, Wiley, New York, 1998.
[53] R. Paternoster, The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues, Justice Quarterly 4, 1987, pp. 173–217.

[54] R. Paternoster, P. Mazerolle, The general strain theory and delinquency: a replication and extension, Journal of Research in Crime and Delinquency 31 (3), 1994, pp. 235–263.
[55] R. Power, 1999 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, Winter 1999.
[56] R. Power, Tangled web: Table of digital crime from the shadows of cyberspace, Que/Manmillan, New York, NY, 2000.
[57] G.E. Reed, P.C. Yeager, Organizational offending and neoclassical criminology: challenging the reach of a general theory of crime, Criminology 34, 1996, pp. 357–382.
[58] R. Rosenthal, R.L. Rosnow, D.B. Rubin, Contrasts and Effect Sizes in Behavioral Research: A Correlational Approach, Cambridge University Press, New York, 2000.
[59] R.J. Sampson, J.H. Laub, Crime in the Making: Pathways and Turning Points through Life, Harvard University Press, Cambridge, MA, 1992.
[60] J.L. Schaub, K.D. Biery, The Ultimate Computer Security Survey, Butterworth Heinemann, Newton, MA, 1995.
[61] J.F. Shoemaker, The Theories of Delinquency, Oxford University Press, Oxford, 1990.
[62] M. Siponen, A conceptual foundation for organizational information security awareness, Information Management & Computer Security 8 (1), 2000, pp. 31–41.
[63] D.A. Smith, P.R. Garton, Specifying specific deterrence, American Sociological Review 54, 1989, pp. 94–106.
[64] D.W. Straub, Effective IS security: an empirical study, Information Systems Research 1 (3), 1990, pp. 255–276.
[65] D.W. Straub, D.L. Goodhue, Security concerns of system users: a study of perceptions of the adequacy of security, Information and Management 20 (1), 1991, pp. 13–27.
[66] D.W. Straub, W.D. Nance, Discovering and disciplining computer abuse in organizations: a field study, MIS Quarterly 14 (1), 1990, pp. 45–62.
[67] D.W. Straub, R. Welke, Coping with systems risk: security planning models for management decision-making, MIS Quarterly 22 (4), 1998, pp. 441–469.
[68] D. Thompson, 1997 Computer crime and security survey, Information Management & Computer Security 6 (2), 1998, pp. 78–101.
[69] H.C. Triandis, Attitude and Attitude Change, Wiley, New York, 1971.
[70] R. von Solms, Information Security Management: why standards are important, Information Management & Computer Security 7 (1), 1999, pp. 50–57.
[71] C.C. Wood, Effective Information Security Management, Elsevier, Oxford, UK, 1991.
[72] http://www.emarketer.com/ereports/eprivacy_security/welcome.html, 2001.

Sang M. Lee (slee1@unl.edu) is the University eminent scholar, regents distinguish professor, and Chair of the Management Department at the University of Nebraska-Lincoln. He has published fifty books and over 200 journal articles in the areas of MIS, management science, operation management, and global business. His current research interests deal with the strategic use of ICT for inter-organizational collaboration.

Sang-Gun Lee (sglee@unlserve.unl.edu) is a research fellow at Sogang University, Seoul, Korea. He received a PhD in MIS from the University of Nebraska-Lincoln. He did part of his doctoral work at Waseda University in Japan. He has published articles in *International Journal of Production Research*, *International Journal of Management Science*, *Journal of MIS Research*, and *Korean Management Science Review*, and presented more than 20 referred papers at HICSS, DIISM (IFIP), AMCIS, DSI, and IRMA.

Sangjin Yoo (yoosj@kmu.ac.kr) is a professor of MIS at Keimyung University in Daegu, Korea. He received a PhD in MIS from the University of Nebraska-Lincoln. Prior to his current position, he was an assistant professor of MIS at Bowling Green State University in Ohio, USA. He has published more than 50 papers in national and international journals including *California Management Review*, *Long Range Planning*, *Organizational Dynamics*, *The Journal of MIS Research*, and *Korean Management Science Review*.