Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2013 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-18-2013

Examining How the Disclosure of IS Security Policies Affect IS Personnel Ethical Conducts

Cathy S. Lin
National University of Kaohsiung, cathy@nuk.edu.tw

Sheng Wu
Southern Taiwan University of Science and Technology, shengwu@mail.stust.edu.tw

EXAMINING HOW THE DISCLOSURE OF IS SECURITY POLICIES AFFECT IS PERSONNEL ETHICAL CONDUCTS

Cathy S. Lin, Department of Information Management, National University of Kaohsiung, Kaohsiung, Taiwan, R.O.C., cathy@nuk.edu.tw

Sheng Wu, Department of Information Management, Southern Taiwan University of Science and Technology, Tainan, Taiwan, R.O.C., shengwu@mail.stust.edu.tw

Abstract

The issue of "professional ethics" in the workplace has been put under the spotlight in recent years; especially several scandals have involved questionable behaviour on the part of information systems (IS) professionals. In the past years, many countries have constructively paid attention to the rules of professional ethics. Among these efforts, many acts asked for corporate information disclosures, for example, the disclosure of IS security and privacy policies.

In this study, two research questions are explored. The first of these investigates the disclosure of IS security policies and perception of codes in Taiwan IS corporations. The second empirically validates a research model to understand whether the disclosure of IS security policies have any influence on the IS professionals' perceptions of codes, and in turn, how these perceptions impact their ethical and unethical conducts. Finally, the theoretical and practical implications to the management of ethics concerning information ethics are discussed.

Keywords: *IS Personnel, Perception of Codes, Information Disclosure, IS Security, Ethical Conducts*

1. INTRODUCTION

The issue of “professional ethics” in the workplace has been in the spotlight in recent years, especially since several enormous incidents have been exposed. Prime examples include the Enron debacle at the end of 2001, as well as a series of scandals perpetrated by Arthur Andersen Accounting in March 2002, WorldCom in April 2002, Merrill Lynch in May 2002, Parmalat Italy in 2003, and Rebar Asia Pacific Group in Taiwan at the end of 2006. These incidents have revealed that the problem concerning business ethics is never a corporate-level problem. These scandals have brought negative externality as different political, social, cultural, and economic environments result in different corporate structures, and these structural conflicts trigger different professional ethical dilemmas. In the past years, many countries have constructively paid attention to addressing this issue; for example, they have placed emphasis on the responsibilities of top and middle levels of management, asked for corporate information disclosures, enhanced professional obligations, and reinforced corporate governance. Among these efforts, the Sarbanes-Oxley (SOX) Act of 2002 in the United States is one of the most prominent regulations. In short, the above-mentioned scandals, domestic as well as foreign, have currently placed the issue of professional conduct of business under special attention.

Just as Gellerman (1989) contends, "Ethics must be managed .... Setting a high moral tone at the top levels of management is necessary" (p. 74). For example, the SOX Act aims at the responsibilities of top and middle levels of management and the obligations of professionals in corporations. The so-called professionals, due to the nature of their occupation, have to govern themselves with higher moral standards than other employees to avoid abusing their authority, which may cause damage to others. This is true for doctors, lawyers, accountants, and even information systems (IS) professionals, as well as myriad other professionals. Especially several scandals have involved questionable behaviour on the part of IS professionals (Davison, Martinsons, Lo, & Kam, 2006). This is very alarming given the extent to which the fast pace of information technology has complicated matters considerably and amplified the scope of “ethical gray areas” (Pastore, 1993). For instance, new information ethics related to intellectual property rights, privacy, and information abuse have emerged due to the fact that information can be easily copied, stolen, and infected. This opportunity is particularly obvious to IS professionals, who observe that unethical behaviors in the workplace can happen effortlessly with only a few keystrokes. Therefore, the ethical dilemmas faced by IS professionals in the workplace embrace not only personal behaviour but also “professional ethics”. To explore the professional obligations of IS personnel, it is necessary to understand the related policies concerning professional ethics at the workplace and how these principles affect employee perceptions and behaviors so as to minimize illegal or unethical conducts.

Therefore, this paper investigates two research studies: The first one investigates the disclosure of IS security policies and perception of codes in Taiwan IS corporations. The second one is to empirically validate a research model to understand whether the disclosure of IS security policies have any influence on IS professionals' perceptions of codes, and in turn, how these perceptions impact their ethical and unethical conducts.

2. LITERATURE REVIEW AND HYPOTHESES

2.1. Disclosure of IS Security Policies

Recent enterprise scandals reveal that there are still many problems related to business practices. To respond to these incidents, for example, the U.S. government has introduced new legislation – the Sarbanes-Oxley (SOX) Act of 2002, which is the most important piece of legislation affecting corporate governance and financial information disclosure. This act coerces corporations to provide transparent and public financial information in order to eliminate possible conflicts of interest between managers and stakeholders. The act has clearly benefited stakeholders by driving greater transparency and improving corporations' internal control systems, which aim at the “disclosure of information”, and increasing the information reliability and accuracy of this effort. Henceforth, the

requirements of information disclosure and information accuracy/reliability are no longer the scope of corporate self-governance but are written professional obligations.

The advocacy about disclosure of information is also the tendency toward social responsibility. For example, the Organisation for Economic Co-operation and Development's Declaration and Decisions on International Investment and Multinational Enterprises comprises ten principles, therein containing clear guidance for information disclosure. According to this document, "enterprises should ensure that timely, regular, reliable and relevant information is disclosed regarding their activities, structure, financial situation and performance" (OECD, 2000), including codes of conduct, and information on the social, ethical, and environmental policies of the enterprise.

Moreover, discussions concerning information accuracy, reliability, and currency have been mentioned in previous studies, rooted in the concept of information quality, which refers to the user's perception of information, that is, evaluation of the output of information systems. For example, Wixom and Todd (2005) examine the variables of information quality and system quality from related research (Bailey & Pearson, 1983; Doll & Torkzadeh, 1988; Jansen & Von Glinow, 1985). Information accuracy represents the user's perception that the information is correct, whereas reliability is related to the dependability of system operation, and currency refers to the user's perception of the degree to which the information is up to date.

While the disclosure of information and information quality becoming a focal point in the ear of information society, this study examines corporations' disclosures of IS security policies. Through the investigation of the disclosure status quo, it would be of help to understand the degree that companies disclose there IS security policies to comply with the social responsibility.

2.2. Perception of Codes

IS professionals often play the role of the gatekeepers in guarding information in business practices; they therefore inevitably have the responsibility to act ethically in the related practices. To regulate the course of actions of IS professionals, businesses often develop a series of codes of conduct governing their behaviour. For example, a code of ethics is treated as an effective method (Frankel, 1989) and constitutes the most commonly adopted program in businesses. The United States systematically incorporated codes of ethics into contemporary society in 1990; at that time, computers were gradually replacing manpower, and IS professional responsibility had increasingly been requested by the corporations and society.

Previous studies have examined the regulatory effects of codes on individual behaviors. However, most of these studies are focused on the influence of the presence or absence of codes of conduct on individual behaviours, and the findings have often been inconsistent. Some studies propose that codes have a positive influence on individual ethical behaviours and suppress unethical one. They generally view the "codes of ethics" as the most feasible way to deal with ethical issues, preventing employees from committing inappropriate actions (Anderson, Johnson, Gotterbarn, & Perrolle, 1993; Khazanchi, 1995; Robin & Reidenbach, 1987; Straub & Nance, 1990). For example, Kreie and Cronan (2000) point out those businesses that have formulated codes of ethics better facilitate their employees to make their own ethical decisions and help them understand whether their behaviours are ethical or unethical. Harrington (1996) points out that the purpose of information ethics codes is to clarify information personnel's responsibilities and to provide certain behavioural guidance for those who face ethical choices. Oz (1992) states that the perception of codes of ethics helps to prevent unethical behaviours from occurring. McCabe, Trevino, and Butterfield (1996) show that the existence of a corporate code of ethics is associated with significantly lower levels of self-reported unethical behaviour in the workplace.

In contrast, other studies show that there is not always a significant relationship between codes and behaviours. For example, Leugenbiehl (1983) states that codes are just texts of advice that may not have specific influences on behaviours. Some studies point out that the influences of codes on behaviours are not absolute. For example, common corporate codes have no significant influences on ethical behaviours, but certain professional codes do (Fimbel & Burstein, 1990; Harrington, 1996;

Somers, 2001). Vitell and Davis (1990) also point out that there is no significant relationship between codes and unethical behaviours.

In summary, the results of previous studies concerning the influences of codes on behaviours are indeed inconsistent. The present study takes a step further and proposes that an individual's "perception of codes" would be the more appropriate factor to truly influence one's behaviours. Just as stated by Stevens (1994) in the discussion over the actual effects and functions of codes, instead of the mere existence of codes, what is far more important is whether employees are aware of the codes of ethics in a corporation and are able to internalize them as guidance for their daily routines and decision-making processes. A similar kind of statement on individual perceptions, the concept of "perceived importance of an ethical issue" (PIE), is also proposed by (Robin, Reidenbach, & Forrest, 1996), who state that an individual's perceived importance of ethical topics belongs to the domain of individual cognition, and the level of perceived importance varies along with individual cognition, including each person's unique ethical sensitivity, the level of moral development, and organizational and individual values.

A concept that is similar to individual perception, as proposed by Trevino (1986), is that individual variables can "influence the likelihood of an individual's acting on the choice of what is thought to be right or wrong" (p. 609). In summary, the concept of an "individual's internal perception" should be an important variable when discussing ethics because this concept is an idiosyncratic process of interpretation, a process of making sense of a complex world in order to plan, choose, and act in that world (Thomas, 1981).

Moreover, this kind of individual perception is influenced by corporate policies, such as codes of ethics and values from the corporate culture Robin et al. (1996). Taking these studies into consideration, the present study broadly defines the construct "perception of codes" to include how one perceives the influence of general corporate codes, information codes of ethics, and codes of practice for information security on one's daily routines or decision making. Furthermore, this study proposes that this kind of code perception may be influenced by the disclosure if IS security policies (hypotheses 1). The discussion on this part will help provide important insights for codes rather than focusing only on the existence or absence of codes.

2.3. Ethical and Unethical Conducts

Different from common criminals, the damage that results from deliberate, illegal behaviors committed by IS professionals is often more severe and extensive. In terms of information-related crimes, Banerjee, Cronan, and Jones (1998) point out that only 1 out of every 100 computer fraud cases are detected, and only 1 out of every 8 detected cases of fraud are disclosed. Moreover, only 3 perpetrators out of every 100 prosecutions are declared guilty, showing how difficult it is to detect information crimes. Furthermore, the illegal behaviours that information personnel are capable of are actually "maximum damage with minimum actions". In other words, a few clicks on the keyboard and ill-intentioned use of computers and the Internet could potentially wreak major havoc on businesses and society.

In previous studies on ethical behaviours, Bommer, Gratto, Gravander, and Tuttle (1987) have proposed a comprehensive behavioural model of ethical/unethical decision making, which points out that an individual's cognitive process may result in two possible behaviours: ethical behaviour and unethical behaviour. For example, Hilton (2000) conducted a survey of Fortune 500 companies to find individual ethical cognition in non-management personnel, or information workers, in information departments. Vitell and Davis (1990) focus on information personnel and discuss individual ethical beliefs and the frequency and opportunities to act unethically. In addition, dedicated surveys target information workers that discuss ethics-related topics such as illegal software duplication (Taylor & Shim, 1993) and e-mail privacy (Cappel, 1995). Robin et al. (1996) propose a model of experimental study focusing on the PIE concept and state that a person's cognition influences that person's behaviours.

Based upon the aforementioned review of academic literature and business practices, this study investigates two research issues: (1) examining the status quo of the disclosure IS security policies and the perceptions of codes; and (2) empirically validating the research model (as shown in Figure 1). In this model, the disclosure of IS security policy claims to have influenced on IS personnel perception of codes (hypotheses 1). In turn, the perceptions of codes have an impact on IS personnel ethical and unethical conducts (hypotheses 2 and 3).

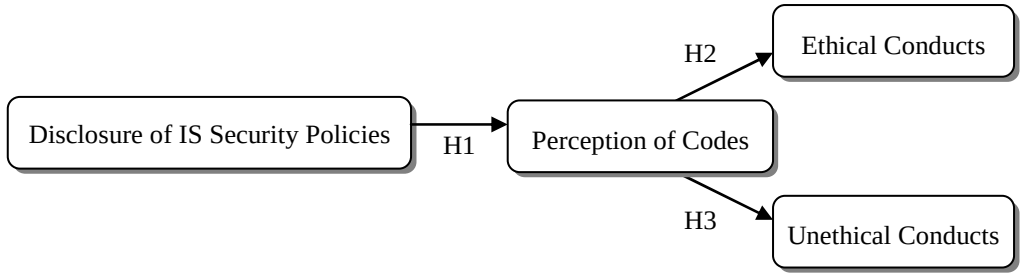

Figure 1. Research Model

3. RESEARCH METHODOLOGY

Previous studies have focused on the importance of asking IS personnel to comply with ethical standards (Couger, 1989; Mason, 1986; Oz, 1992). Research also has suggested that students in the information field should cultivate appropriate ethical values in order to meet future occupational demands. However, only a handful of these studies have focused on collecting data from IS personnel. Thus, we have adopted a field survey for conducting the present study. The data collected from IS personnel would be useful for understanding current business practices and how their perception of codes would be influenced by the disclosure of IS security policies; further, it is also helpful for understanding how their perceptions of codes have impacted their ethical and unethical conducts.

3.1. Subjects

The participants in this study were IS personnel working in the Information Technology industry. This study initially contacted managers of Information Technology departments or senior Information Technology personnel in Taiwan to ask for their participation in this study. We told all participants that their responses would be kept confidential and only summary information would be presented. We also assured them of complete anonymity. The exclusion of incomplete questionnaires resulted in a total of 116 usable responses. As shown in Table 1, among these respondents, 75.00% were male and 25.00% were female. The age of the respondents ranged from 30 to 54 years old. On average, respondents had a working seniority of 11.40 years. Table 1 details the respondents' characteristics.

Demographic Variable	**Sample Composition**	
Gender	Male: 87 (75.00%); Female: 29 (25.00%)	
Age (year)	Mean = 36.02; Std = 4.78; Range: 30~54	
Work Experience (year)	Mean = 11.40; Std = 5.30; Range: 2~29	
Job Title	Chief Information Officer	10 (8.62%)
	Systems Analyst	28 (24.14%)
	System Engineer	18 (15.52%)
	Programmer	33 (28.45%)
	Web Administrator	7 (6.03%)

Demographic Variable	Sample Composition		
	Others	21	(17.24%)

Table 1. Sample Demographics (N=116)

3.2. Measurement Development

Four constructs were measured: disclosure of IS security policies, perception of codes, ethical conducts, and unethical conducts. Constructs were measured using a multiple-item scale drawn from pre-validated studies and reworded to relate specifically to this study. The applicability of the modified items was enhanced by literature reviews, using two MIS professors as expert judges, and pretested using twenty IS personnel. During this process, scale items were trimmed and refined, and dimensions were modified to maintain the content validity as our understanding of the constructs improved. The research construct of the disclosure of IS security policies is an actual state measure of the policies disclosure concerning IS security, anchored with 5-point likert scale from "no disclosure" to "clear disclosure". The perception of codes is a subjective measure about how the codes influence individuals in dealing with the daily tasks or making decisions, anchored with 10-point likert scale from "no influence" to "complete influence". As for the other two constructs anchored with 7-point from "strongly disagree" to "strongly agree". Table 2 shows the questionnaire items and sources of measurement of variables.

Constructs	Measurement Items	Source
Disclosure of IS Security Policies *(5-point Likert scales)*	Our company has actualized the investment and training related to information security management.	MOEA (2003)
	Our company has units dedicated to information security management.	
	Our company has formulated standards or guidance regarding the practices of information security management.	
	Our company has policies and performance criteria regarding the evaluation of information security management.	
	Our company regularly announces specific information regarding information security management.	
	Our company announces information security management mechanisms in reports or on the company website.	
Perception of Codes *(10-point Likert scales)*	Please evaluate how the "company codes" influence you dealing with the daily tasks or making decisions.	Somers (2001)
	Please evaluate how the "IS security policies" in your company influence you dealing with the daily tasks or making decisions.	
Ethical Conducts *(7-point Likert scales)*	Being IS personnel, my professional conduct must be guided by the adherence to all applicable laws and regulations.	Singhapakdi and Vitell (1993)
	Being IS personnel, I never manipulate the availability of a product for purpose of exploitation.	
	Being IS personnel, I meet obligations and responsibilities in contracts and mutual agreements in a timely manner.	

Constructs	Measurement Items	Source
Unethical Conducts *(7-point Likert scales)*	In order to succeed in my company, it is often necessary to compromise one's ethics.	Vitell and Davis (1990)
	Successful IS personnel in my company withhold information that is detrimental to their self-interest.	
	Successful IS personnel in my company look for a "scapegoat" when they feel they may be associated with failure.	
	Successful IS personnel in my company take credit for the ideas and accomplishments of others.	

Table 2. Measurement Items

3.3. Reliability and Validity

The partial least squares model was employed to test our measurements and proposed hypotheses. The SmartPLS 2.0 M3 (Ringle, Wende, & Will, 2005), which has also been frequently adopted in many information systems journals such as MIS Quarterly (Brown & Venkatesh, 2005; Furneaux & Wade, 2011; Siponen & Vance, 2010), was employed for this analysis. Item reliability, convergent validity, and discriminant validity tests are often used to evaluate the measurement model in PLS. Reliability can be assured through composite reliability (CR), alpha, and factor loading. Factor loadings higher than 0.7 may be viewed as highly reliable, whereas factor loadings lower than 0.5 should be dropped. Table 3 demonstrates that all the Cronbach's alpha values fall between 0.84-0.95, CR values fall between 0.89-0.96, and factor loadings values fall between 0.78-0.95 (see Table 3).

Constructs	Items	Factors loading	Cronbach *α*	CR	AVE
Disclosure of Information Security Policy (DISP)	DISP1	0.90	0.95	0.96	0.81
	DISP 2	0.94			
	DISP 3	0.95			
	DISP 4	0.94			
	DISP 5	0.89			
	DISP 6	0.78			
Ethical Conducts (EC)	EC1	0.91	0.84	0.89	0.73
	EC2	0.80			
	EC3	0.86			
Unethical Conducts (UC)	UC1	0.83	0.89	0.92	0.75
	UC2	0.84			
	UC3	0.91			
	UC4	0.88			
Constructs	**Items**	**Weights**	**Cronbach *α***	**CR**	**AVE**
Perception of Codes (PC)*	PC1	0.09	na	na	na
	PC2	1.05			

Constructs	Items	Factors loading	Cronbach α	CR	AVE
* Perception of Codes is a formative variable, therefore no reliability and validity is calculated.					

Table 3. Reliability, validity and correlation matrix

Convergent validity should be assured when multiple indicators are used to measure one construct. This can be examined by CR and averaged variance extracted (AVE) by constructs (Fornell & Larcker, 1981). For convergent validity to be necessary, CR should be higher than 0.7, and AVE should be higher than 0.5. Table 3 demonstrates that all the AVE values fall between 0.73-0.81. For discriminant validity to be required, the correlation between construct pairs should be lower than 0.90 and the square root of AVE should be higher than the interconstruct correlation coefficients (Fornell & Larcker, 1981). Data shown in Tables 4 indicate that all minimum requirements were met; therefore, the results exhibit strong construct reliability and validity.

Constructs	Descriptive Statistics		Correlation between Constructs			
	Mean	Std.	DISP	EC	UC	PC
DISP	3.40	1.17	***0.81***			
EC	6.40	0.67	0.31	***0.73***		
UC	2.35	1.23	-0.35	-0.36	***0.75***	
PC	6.89	2.05	0.50	0.34	-0.24	***na***
Diagonal elements represent the average variance extracted (AVE), and off-diagonal elements represent the correlations among constructs. All correlations are significant at the 0.01 level (2-tailed).						

Table 4. Descriptive Statistics and Discriminant validity for the research constructs

4. DATA ANALYSIS AND RESULTS

4.1. Investigating the Disclosure of IS Security Policies and Perception of Codes

To answer the first research question, table 5 shows the result of investigating the disclosure of IS security policies, which items are adopted from the Ministry of Economic Affairs (MOEA) in Taiwan. The results indicate that 89.7% of the businesses had carried out the investment and training related to information security management, 86.2% of the businesses had units dedicated to the practices of information security management, 87.9% of the businesses formulated standards or guidance regarding the practices of information security management, 83.7% of the businesses had policies and performance criteria regarding the evaluation of information security management, 80.2% of the businesses regularly announced specific information regarding the practices of information security management, and 75.8% of the businesses announced information security management mechanisms in reports or on the company website.

Disclosure of Information Security Policy	Has carried out	Has not carried out	Don't Know
1. Our company has actualized the investment and training related to information security management.	89.7%	3.4%	6.9%
2. Our company has units dedicated to the practices of information security management.	86.2%	1.7%	12.1%

Disclosure of Information Security Policy	Has carried out	Has not carried out	Don't Know
3. Our company has formulated standards or guidance regarding the practices of information security management.	87.9%	2.6%	9.5%
4. Our company has policies and performance criteria regarding the evaluation of information security management.	83.7%	3.4%	12.9%
5. Our company regularly announces specific information regarding the practices of information security management.	80.2%	3.4%	16.4%
6. Our company announces information security management mechanisms in reports or on the company website.	75.8%	2.6%	21.6%

Table 5. Investigation of the disclosure IS security policies

In investigating the current business practices concerning setting up the codes of conduct, this study adapted the measurement item from Somers (2001), which inquires whether the company had published corporate codes for employees. In this study, we extended this item to two kinds of codes and ask the respondents how the codes of conducts (including general corporate codes and codes of practice for IS security policies) influence IS personnel dealing with the daily tasks or making decisions. The result was shown in Table 6.

Types of Codes	Min	Max	Mean	Std
1. Please evaluate how the "company codes" influence you dealing with the daily tasks or making decisions.	1	10	6.35	2.26
2. Please evaluate how the "IS security policies" in your company influence you dealing with the daily tasks or making decisions.	1	10	7.47	2.22

Table 6. Investigation of the perception of codes

4.2. Model Validation Results

The second research question is to validate the proposed model as shown in figure 1. In this paper, we assessed the hypotheses by using structural equation modelling because of its ability to validate multiple causal relationships simultaneously. SmartPLS 2.0 M3 with bootstrapping as a resampling technique (500 random samples) was used to estimate the structural model and the significance of the paths (Chin, 1998). Path coefficients (t value) and the R^2 were used jointly to evaluate the model. With the hypotheses being unidirectional, statistical tests were assessed at the 5 percent level of significance using a two-tailed t-test. Figure 2 shows the structural model. The research findings show that all the three hypotheses were statically significant.

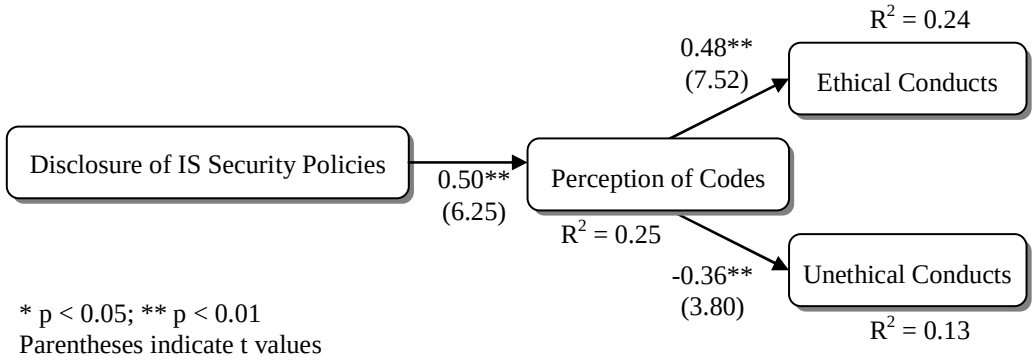

Figure 2. Model Result

First, hypothesis 1 examines the links between disclosure of IS security policies and the perception of codes in company. Disclosure of IS security policies is significantly associated with the perception of codes (β=0.50, t-value=6.25). The disclosure of IS security policies explains the 25% variance of perception of codes. Hence, H1 is supported. Second, the perception of codes both have impacted on ethical conducts (β=0.48, t-value=7.52) and unethical conducts (β=-0.36, t-value=3.80). Therefore, H2 and H3 are supported. All the explanatory power in this study is greater than the recommended level of 10% (Falk & Miller, 1992; Phang et al., 2006). In sum, the findings in this study demonstrate that businesses disclose their IS security policies will be of help for IS personnel in strengthening their perception of codes, and such perception will in turn play a role that guides them to behave ethically and avoid unethical acts.

5. CONCLUSIONS

This unique of this study is that the first research question helps telling the status quo of the IS security policies disclosure, which is a kind of objective investigation. Therefore the actual state is treated as the antecedent of this research model; so as to further understand if the current disclosure sate of play will have influence on individual's subjective perception of codes, in turn, impact on ethical and unethical acts.

This study discusses the importance of the disclosure of IS security policies on IS personnel perception of codes from the perspective of "professional ethics". This study found that IS security policies have significant influences on information personnel's code perception. Moreover, individual code perception also has a significant influence on ethical or unethical conducts. Different from past studies that focused on the existence or absence of codes, this study took a step further and discovered that individual code perception is a variable that truly influences individual behaviours. Furthermore, the inspection of the cognition and behaviours in the IS personnel who work in Taiwan's information corporations is an important referent.

References

Anderson, R. E., Johnson, D. G., Gotterbarn, D., & Perrolle, J. (1993). Using the new ACM code of ethics in decision making. Communications of the ACM, 36(2), 98-107.

Bailey, J. E., & Pearson, S. W. (1983). Development of a tool for measuring and analyzing computer user satisfaction. Management science, 29(5), 530-545.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: a study in situational ethics. Mis Quarterly, 22(1), 31-60.

Bommer, M., Gratto, C., Gravander, J., & Tuttle, M. (1987). A behavioral model of ethical and unethical decision making. Journal of Business Ethics, 6(4), 265-280.

Brown, S. A., & Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. MIS Quarterly, 399-426.

Cappel, J. J. (1995). A study of individuals' ethical beliefs and perceptions of electronic mail privacy. Journal of Business Ethics, 14(10), 819-827.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. MIS Quarterly, 22(1), vii-xvi.

Couger, J. D. (1989). Preparing IS students to deal with ethical issues. Mis Quarterly, 211-218.

Davison, R. M., Martinsons, M. G., Lo, H. W., & Kam, C. S. (2006). Ethical values of IT professionals: evidence from Hong Kong. Engineering Management, IEEE Transactions on, 53(1), 48-58.

Doll, W. J., & Torkzadeh, G. (1988). The measurement of end-user computing satisfaction. Mis Quarterly, 12(2), 259-274.

Falk, R. F., & Miller, N. B. (1992). A primer for soft modeling: University of Akron Press.

Fimbel, N., & Burstein, J. S. (1990). Defining the ethical standards of the high-technology industry. Journal of Business Ethics, 9(12), 929-948.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.

Frankel, M. S. (1989). Professional codes: Why, how, and with what impact? Journal of Business Ethics, 8(2-3), 109-115.

Furneaux, B., & Wade, M. (2011). An Exploration of Organizational Level Information Systems Discontinuance Intentions. Management Information Systems Quarterly, 35(3), 573-598.

Gellerman, S. W. (1989). Managing ethics from the top down. Sloan Management Review, 30(2), 73-79.

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.

Hilton, T. (2000). Information systems ethics: a practitioner survey. Journal of Business Ethics, 28(4), 279-284.

Jansen, E., & Von Glinow, M. A. (1985). Ethical ambivalence and organizational reward systems. Academy of Management Review, 10(4), 814-822.

Khazanchi, D. (1995). Unethical behavior in information systems: the gender factor. Journal of Business Ethics, 14(9), 741-749.

Kreie, J., & Cronan, T. P. (2000). Making ethical decisions. Communications of the ACM, 43(12), 66-71.

Leugenbiehl, H. C. (1983). Moral Education and the Codes of Ethics. In V. Weil (Ed.), Beyond Whistleblowing: Defining Engineers' Responsibilities (pp. 284-299). Chicago: Illinois Institute of Technology.

Mason, R. O. (1986). Four ethical issues of the information age. Mis Quarterly, 5-12.

McCabe, D. L., Trevino, L. K., & Butterfield, K. D. (1996). The influence of collegiate and corporate codes of conduct on ethics-related behavior in the workplace. Business Ethics Quarterly, 6(4), 461-476.

MOEA. (2003). Principles for Responsible Investment. Department of Investment and Services of Ministry of Economic Affairs, from http://csr.moea.gov.tw/articles/articles_content.asp?ar_ID=1076

OECD. (2000). The OECD Declaration and Decisions on International Investment and Multinational Enterprises: Basic Texts, from http://www.olis.oecd.org/olis/2000doc.nsf/4f7adc214b91a685c12569fa005d0ee7/c125692700623b74c1256991003b5147/$FILE/00085743.PDF

Oz, E. (1992). Ethical standards for information systems professionals: A case for a unified code. Mis Quarterly, 16(4), 423-433.

Pastore, R. (1993). Ethical Gray Matters. CIO, 58-62.

Phang, C. W., Sutanto, J., Kankanhalli, A., Li, Y., Tan, B. C. Y., & Teo, H. H. (2006). Senior citizens' acceptance of information systems: A study in the context of e-government services. IEEE Transactions on Engineering Management, 53(4), 555-569.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0. Hamburg. Retrieved from http://www.smartpls.de

Robin, D. P., & Reidenbach, R. E. (1987). Social responsibility, ethics, and marketing strategy: closing the gap between concept and application. The Journal of Marketing, 44-58.

Robin, D. P., Reidenbach, R. E., & Forrest, P. (1996). The perceived importance of an ethical issue as an influence on the ethical decision-making of ad managers. Journal of Business Research, 35(1), 17-28.

Singhapakdi, A., & Vitell, S. J. (1993). Personal and professional values underlying the ethical judgments of marketers. Journal of Business Ethics, 12(7), 525-533.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.

Somers, M. J. (2001). Ethical codes of conduct and organizational context: A study of the relationship between codes of conduct, employee behavior and organizational values. Journal of Business Ethics, 30(2), 185-195.

Stevens, B. (1994). An analysis of corporate ethical code studies:“Where do we go from here?”. Journal of Business Ethics, 13(1), 63-69.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. Mis Quarterly, 45-60.

Taylor, G. S., & Shim, J. P. (1993). A comparative examination of attitudes toward software piracy among business professors and executives. Human Relations, 46(4), 419-433.

Thomas, K. (1981). Comparative Risk Perception: How the Public Perceives the Risk and Benefits of Energy Systems. Paper presented at the Proceedings of the Royal Society of London.

Trevino, L. K. (1986). Ethical decision making in organizations: A person-situation interactionist model. Academy of Management Review, 11(3), 601-617.

Vitell, S. J., & Davis, D. L. (1990). Ethical beliefs of MIS professionals: The frequency and opportunity for unethical behavior. Journal of Business Ethics, 9(1), 63-70.

Wixom, B. H., & Todd, P. A. (2005). A theoretical integration of user satisfaction and technology acceptance. Information Systems Research, 16(1), 85-102.