Asia Pacific Journal of Information Systems
Vol. 26 No. 1 (MARCH 2016), 163-188

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
http://dx.doi.org/10.14329/apjis.2016.26.1.163

Intentions of Employees to Whistleblow Information Security Policy Violations in the Organization

Wei, Liang-Cheng[a], Carol Hsu[b*], Kai Wang[c]

[a] *Application Consultant, IBM, Taiwan*
[b] *Professor, Department of Information Management at National Taiwan University, Taiwan,*
[c] *Associate Professor, Chairman of Department of Information Management at National University of Kaohsiung, Taiwan*

ABSTRACT

Compliance with information security policies has been an important managerial concern in organizations. Unlike traditional general deterrent theory, this study proposes whistle-blowing as an alternative approach for reducing internal information security policy violations. We build on the theories of planned behavior and rational choice as well as develop a theoretical model to understand the factors that influence whistle-blowing attitudes and intention at both the organizational and individual levels. Our empirical results reveal that altruistic and egoistic concerns are involved in the development of whistle-blowing attitudes. The results not only extend our understanding of whistle-blowing motivation but also offer directions to managers in promoting internal disclosure of information security breaches.

Keywords: Information Security Policy Violation, Internal Whistleblowing, Behavioral Issues Of Information Security, Theory Of Planned Behavior, Rational Choice Theory

Ⅰ. Introduction

Information security management has been an important management agenda in modern organizations. In particular, insider threat has become a major source of information security breaches. According to Symantec's (2012) report, 40.6% of data breaches are due to hacker attacks, whereas 48.2% of data breaches are caused by insider abuse because of either employee malfeasance or employee negligence. Furthermore, Herath and Rao (2009) argue that regulating employee behavior is difficult and the conventional surveillance approach can be "extremely costly and may not be even practically possible" (Herath and Rao, 2009, p. 195). In addition, the current implementation of technical monitoring mechanisms cannot detect all wrongdoings.

Thus, this study proposes whistleblowing as an

*Corresponding Author. E-mail: carolhsu@ntu.edu.tw Tel: 886233661196 alternative approach to complement and reinforce existing information security protection against insider security breaches. The mechanism of whistleblowing has been designed in organizational literature to encourage employees to speak up and inform on others' unethical practices. This stream of literature elucidates the motivational mechanisms upon which whistleblowers depend on when formulating their judgments and decisions. Within the information systems (IS) literature, the whistleblowing perspective has been employed in the context of information technology (IT) project management (Park et al., 2008; Park and Keil, 2009; Smith et al., 2001). To the best of our knowledge, for information security management, we only found the study of Oh and Teo (2010) on the role of whistleblowing as a countermeasure against software piracy in organizations; however, few studies have focused on computer-related incidents (Pierson et al., 2007). In this research, we conceptualize insider security breaches as a form of employee wrongdoings and attempt to address two research questions. (1) What influences employees to whistleblow a perceived violation of information security policy (ISP)? (2) What promotes an employee's attitude toward whistleblowing ISP violations? Through the empirical study, we aim to contribute to managerial and behavioral aspect of information security management by offering insights into employees' motivation in whistleblowing ISP violations. A better understanding of whistleblowing mechanisms can help managers to design a stronger ethical culture for information resource protection within the organization.

This paper is organized as follows. Section 2 reviews the existing literature on employee compliance with information security policies and studies on IT-related whistleblowing. Section 3 discusses our theoretical model. Section 4 describes the methodological approach adopted in this study. Section 5 presents the results. Section 6 discusses the implications and limitations, and Section 7 concludes this study.

Ⅱ. Literature Review

2.1. Employee Compliance with Information Security Policy

As mentioned earlier, ISP compliance has become an important concern in organizations. Building on the general deterrence theory (GDT), D'Arcy et al. (2009) consider IS misuse as a type of criminal act. They examine the deterring effects of three countermeasures—security policy, a security education, training, and awareness (SETA) program, and computer monitoring—on employee intention to misuse IS resources. Siponen and Vance (2010) additionally incorporate "neutralizing techniques" using the GDT approach to explain the psychological patterns adopted by immoral employees who justify their wrongdoings. Herath and Rao (2009) in another study employ the "principal agent paradigm" to model the relation between information security managers and employees. They discover that with the effects of penalties, social pressure, and intrinsic motivation, a considerable amount of variance in employees' intentions to comply with ISP can be explained. Bulgurcu et al. (2010) examine the roles of rationality-based beliefs and information security awareness contributing to employees' decision-making processes prior to determining their compliance intentions with ISP. Johnston and Warkentin (2010) consider communication between security managers and general employees as a "fear appeal" and argue that implicit messages within the persuasion will influence individual intents to adopt the recommended approach. Finally, Hu et al. (2012) examine the preceding effects of "top management support" and "organizational culture" on the attitude, subjective norms, and perceived behavioral control. They analyze the manner in which these constructs influence individual intentions to comply with ISP.

While previous studies have enhanced our understanding of compliance with ISP, these studies have primarily focused on the determinants of end user behavior to obey or violate ISP. However, few studies have discussed the role of employee whistleblowing in information security protection. As elucidated earlier, sometimes it becomes difficult to discover cases and expensive to monitor those cases. Therefore, we propose that rather than merely focusing on information system user behavior, it would be useful to examine employee intention to whistleblow internal ISP violations. The following section discusses the application of whistleblowing in the IS domain.

2.2. IT-Related Whistleblowing

In the IS literature, thehas been applied have applied in the context of IT concept of whistleblowing project management and IT malpractices. Whistleblowing is needed for IT project management mainly because for some enormous IT projects, project leaders might opt to conceal the true project status (or progress) despite huge pressure to match pre-determined schedules. To avoid such unfavorable outcomes and to notify management as early as possible, several studies (e.g., Park et al., 2008; Park and Keil, 2009; Smith et al., 2001; Tan et al., 2003) have examined the whistleblowing mechanism and have investigated the phenomenon why some individuals choose to remain silent on the real status of an IT project, whereas others choose to communicate the bad news up the organizational hierarchy (Park and Keil, 2009). Keil et al. (2010) explain the whistleblowing intention within IT projects based on the argument of benefit-to-cost differential. They argue that a whistleblower's intention to report wrongdoings is strongly associated with the benefits and costs expected to follow their actions. Benefits include the intrinsic and extrinsic rewards arising from the exposure of the wrongdoing, whereas costs mostly center on the retaliation whistleblowers might suffer from other employees (Keil et al., 2010).

Oh and Teo (2010) examine the role of whistleblowing as a countermeasure against software piracy in organizations. They adopt behavioral reasoning theory—an extension of Ajzen's theory of planned behavior (TPB)—to model individuals' external whistleblowing intentions mainly to incorporate the motivational mechanisms upon which whistleblowers depend on when formulating their judgments and decision making. Their empirical findings indicate that the "reasons for" and "reasons against" are both significant predictors of one's attitude and that global motives (attitude, subjective norms, and perceived behavioral control) are significant predictors of one's intention to whistleblow on software piracy. In addition, they find that one is more likely to externally report software piracy when one has a bad relation with the organization and when the perceived level of legal protection is high. Stylianou et al. (2013) conduct the research on whistleblowing in the area of IT malpractices. They discover that female workers are more likely to whistleblow on "intellectual property infringement" and "privacy rights violations." Computer literacy is not found to be significantly related to whistleblowing intention. Machiavellianism has a significant moderating effect not only on the relation between gender and whistleblowing intention but also on the relation between computer literacy and whistleblowing intention. More recently, Lowry et al. (2013) analyze the factors that would influence employees to use a whistleblowing reporting system. They differentiate between traditional means of whistleblowing and system-based whistleblowing. Their empirical results of a scenario-based experiment reveal that perceived risk to the organization and to self are both significant predictors of failure ought to be reported and responsibility to report. Trust in both report-receiving parties and the reporting system is found to contribute to one's willingness to report.

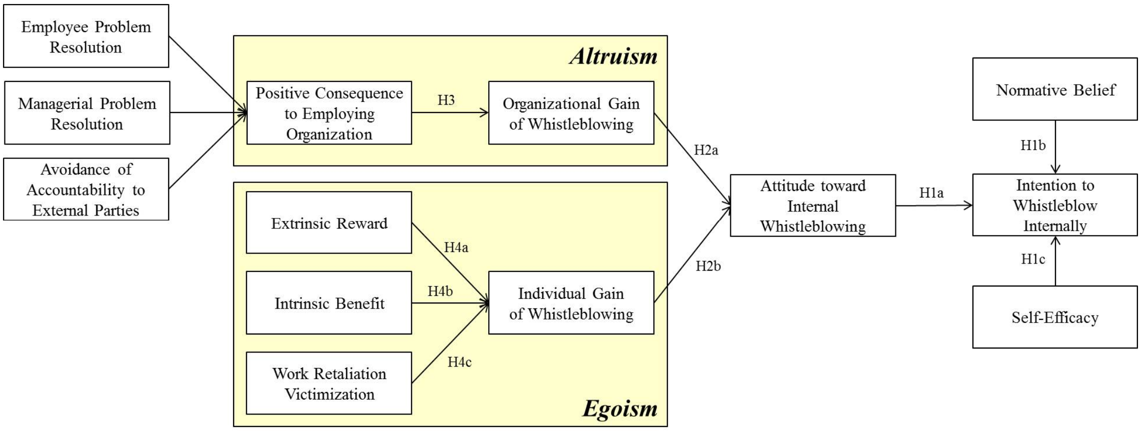
The above studies have highlighted the potential values of whistleblowing in managing IT-related risk at project level and some aspects related to IT misuse. Building on this stream of research, this study aims to develop a more comprehensive framework reflecting benefit and cost concerns underlying a whistleblowing decision for ISP violations. The next section elaborates more on our conceptual framework.

Ⅲ. Conceptual Model

This study adopts TPB as a theoretical foundation to explain employee intention toward whistleblowing within a comprehensive framework. As illustrated In <Figure 1>, an employee's intention to internally report a perceived violation of ISP is influenced by attitude, normative beliefs (the antecedent of subjective norms), and self-efficacy (an equivalent concept to perceived behavioral control). Section 3.1 introduces TPB and delineates the manner in which whistleblowing can be represented as planned behavior. Section 3.2, following a brief review of rational choice theory (RCT), proposes that the decision-making process of whistleblowers can be modeled by a rational evaluation of all the likely consequences of whistleblowing. Finally, Sections 3.3 and 3.4 differentiate these consequences into two levels and link them separately to the overall assessment of organizational and individual gains. Overall, four sets of hypotheses are presented in our theoretical model.

3.1. Theory of Planned Behavior

TPB, originally proposed by Ajzen (1991), is one of the most powerful psychological frameworks adopted by researchers of various disciplines to ex-


Employee Problem Resolution
Managerial Problem Resolution
Avoidance of Accountability to External Parties
Altruism
Positive Consequence to Employing Organization
H3
Organizational Gain of Whistleblowing
H2a
Extrinsic Reward
H4a
Intrinsic Benefit
H4b
Individual Gain of Whistleblowing
Work Retaliation Victimization
H4c
Egoism
H2b
Attitude toward Internal Whistleblowing
H1a
Normative Belief
H1b
Intention to Whistleblow Internally
H1c
Self-Efficacy

<Figure 1> Research Model

plicate the relation between attitude, intention, and behavior. Attitude refers to a person's opinion regarding one's behavior, whereas intention refers to his or her readiness to conduct the given behavior. The former functions as a preceding factor of the latter, whereas the latter serves as the immediate predictor of the actual behavior. Since the measurement of several behaviors in organizational environments is practically impossible or economically infeasible, scholars (e.g., Herath and Rao, 2009; Hu et al., 2012) tend to use intention as a proxy variable for the interested behavior. In this study, we follow this line of thinking and consider behavioral intention as a proxy variable for the actual whistleblowing behavior.

Three major determinants in this framework are believed to impact an individual's behavioral intention. Attitude refers to the degree to which a person approves of one certain behavior. Normative belief refers to the degree to which one believes his or her significant others agree with such planned behavior. Self-efficacy refers to the confidence one has in their own ability to achieve that behavior. Numerous studies have revealed that these three determinants explain a significant amount of variance in behavioral intention. Therefore, it is considered to be one of the most effective psychological frameworks to predict human behavior. Based on the essence of the utilized theoretical framework and the results of the previous empirical tests (e.g., MacNab and Worthley, 2008; Park and Blenkinsopp, 2009; Trongmateerut and Sweeney, 2013) on the intention to whistleblow in the general context, we hypothesize that

H1a: Attitude positively relates to the intention to internally whistleblow ISP violation.

H1b: Normative belief positively relates to the intention to internally whistleblow ISP violation.

H1c: Self-efficacy positively relates to the intention to internally whistleblow ISP violation.

Of the three presented determinants, attitude has been shown to be relatively more important than the other two. Previous studies (e.g., Bulgurcu et al., 2010) have considered attitude as the only variable that can be externally manipulated by objective information. Besides, several derived theories (e.g., technology acceptance model) originating from TPB also primarily focus on attitude. In this empirical investigation, we also attempt to understand the preceding factors of end user attitude in the context of ISP compliance. In TPB, this factor is named behavioral belief and is defined as an individual's subjective evaluation of each likely outcome that might follow the completion of the behavior (Ajzen, 2011). As these outcomes vary from one behavior to another, it is important for researchers to individually extract the salient beliefs from peoples' minds (Ajzen, 2011). To achieve this goal, Ajzen (2011) suggests conducting interviews with a representative sample population for investigating the perceived advantages and disadvantages of the interested behavior to determine a representative set of behavioral beliefs. In other words, people develop a positive or negative attitude toward one certain behavior based on their assessment of likely outcomes as either advantageous or disadvantageous to them. We introduce another framework to complement the current TPB model to further include this rationale.

3.2. Rational Choice Theory

RCT is an economic approach adopted by many economists, sociologists, and political scientists to model human decision-making behavior. The fundamentals of this framework suggest that individuals calculate the expected benefits and costs of a given action before they truly engage in it (Scott, 2000). Exploiting the studies of Paternoster and Pogarsky (2009) and McCarthy (2002), Bulgurcu et al. (2010) propose a procedure to explain the manner in which a person reaches a rational decision. They argue that decision makers first identify alternative courses of action (i.e., possible reactions) in a particular context. Then, they reflect on the likely consequences for each action. Since the underlying assumption of RCT suggests that people have preferences for different outcomes (McCarthy, 2002), each possible outcome of the certain behavior can be labeled as either a benefit or a cost to the decision maker. Next, outcomes that follow a given behavior are grouped by decision makers to conduct an overall appraisal to see how much "utility" will be generated once those outcomes occur. Here, "utility" can denote the net satisfaction or dissatisfaction one will gain from the behavior. With all the utility scores at hand, decision makers are able to compare the "good" of each alternative course of action and choose the alternative that maximizes their gain.

We believe that a linkage exists between TPB and RCT. In TPB, individuals foster their attitudes toward a behavior based on their subjective evaluation of likely outcomes, whereas in RCT, individuals assess the overall utility of outcomes for each alternative so that a decision can be made. Both theories suggest that people contemplate the expected outcomes before actually taking an action. Drawing these two frameworks together, each outcome belief in TPB can be considered as either a benefit or a cost to an individual and that individuals balance these benefits and costs to reach a rational decision with maximum gains. In fact, this incorporation of utilitarian factors as behavioral beliefs into the TPB model coincides with several previous IS studies (e.g., Bock et al., 2005; Bulgurcu et al., 2010; Liao et al., 2010) in which antecedents of attitude are either benefits or costs. Thus, we believe that it is appropriate to denote each outcome belief as either a benefit or cost factor of individual attitudes.

When evaluating the benefit and cost of whistleblowing in the organizational context, Dozier and Miceli (1985) argue that people balance benefits and costs at two levels. At the organizational level, a disclosure of wrongdoings may help the organization to recover from the wrongdoing, but it may also threaten the authority structures (Dozier and Miceli, 1985). At the individual level, whistleblowers may suffer serious retaliation from other employees even though many of them consider that what they did for the organization is morally acceptable.

In theorizing the benefit and cost at these two levels, concerns over organizational gain are associated with altruism (an ethical disposition that intends for others' well-being, regardless of the possible harm to self), whereas concerns over personal gain are associated with egoism (the other inclination that suggests self-interest is the just and proper motive for human activities). However, instead of viewing whistleblowing as a totally selfish (egoistic) or totally unselfish (altruistic) behavior, Dozier and Miceli (1985) suggest that discussing it from a pro-social perspective is more appropriate as the manner in which whistleblowers intervene and halt the perceived wrongdoings comprises both selfish and unselfish elements. Pro-social behavior is defined as a voluntary deed that attempts to help others in the society without ignoring self-interest and practical concerns. Therefore, we argue that a spectrum exists manifesting the level to which the whistleblowing act is out of altruistic motives or egoistic motives. Differentiating these two elements of whistleblowing behavior as the antecedents of individual attitudes, we believe that interesting results might ensue that will explain the balance of altruism and egoism in whistleblowers' minds. Thus, we hypothesize that

H2a: Organizational gain of whistleblowing positively relates to an individual attitude toward internal whistleblowing.

H2b: Individual gain of whistleblowing positively relates to an individual attitude toward internal whistleblowing.

3.3. Altruistic Factors

We employ the conceptual framework proposed by Miceli and Near (1992) to include all the favorable and unfavorable consequences of whistleblowing to further develop altruistic and egoistic factors at the organizational level. Positive consequences of whistleblowing to the employing organization include "increased safety and well-being of organization member," "support for codes of ethics," "reduction of waste and mismanagement," "improved employee morale," "maintenance of good will and avoidance of damage claims," and "avoidance of legal regulation,"; conversely, negative consequences to the employing organization include "challenge to authority structure," "threats to organizational viability," "limits on control," and "unpredictability of organization member actions" (Miceli, 1992).

Each dimension of these two concepts can be put into the information security context to develop a new meaning. For example, given that corrective measures are taken following a whistleblowing report, we argue that employee access to IS resources would be safeguarded, ISP would be more highly valued, the waste and mismanagement regarding IS resource use would be reduced, information security awareness (employee morale) would be raised, the goodwill regarding information security protection would be maintained, and the damage claims and legal sanctions based on IT-related laws would be avoided. In contrast, employee whistleblowing of ISP violations might also challenge the information security governance structure (if the organization climate does not encourage members to speak up), threaten organizational viability (if the organization depends on preventing ISP violations to sustain its profitability), limit other's discretion to utilize IS resources, and increase the likelihood of others abusing whistleblowing mechanisms (if employees hold personal grudges against each other). Since the negative consequences of whistleblowing to the organization only occur under certain and uncommon conditions such as unresponsive managerial attitudes and an unethical organizational climate, this study excludes them from the theoretical models. With these six consequences of whistleblowing inherently being beneficial to the employing organization, we hypothesize that

H3: Positive consequence to the employing organization positively relates to organizational gain of whistleblowing.

3.4. Egoistic Factors

At the individual level, the positive consequence of whistleblowing can be twofold: extrinsic rewards and intrinsic benefits (Keil et al., 2010, p. 790). Extrinsic rewards can be defined as monetary or non-monetary incentives offered by an organization to its employees in the hope of aligning personal interest with organizational goals, whereas intrinsic benefit can be defined as positive feelings arising from personal achievement (Bulgurcu et al., 2010). The former is a widely used approach to encourage desirable practices within organizations, whereas the latter is considered to be a powerful incentive known as "internal motivation." We posit that both can be used to encourage whistleblowing of ISP violations.

Equally, negative consequences of whistleblowing exist at the individual level (Oh and Teo, 2010). These include retaliation against one's working duties as well as one's interpersonal relations (Cortina and Magley, 2003). The former (work retaliation victimization) may appear in forms ranging from punitive transfer and demotion to dismissal, whereas the latter (social retaliation victimization) may appear in the form of peer exclusion (Cortina and Magley, 2003). Theoretically, both discourage whistleblowing of ISP violations. However, this study includes only work retaliation victimization in the proposed model because of some measurement flaws. The following section thoroughly discusses our hypotheses at the individual level.

3.4.1. Extrinsic Rewards

Based on the study by Bulgurcu et al. (2010), extrinsic rewards in the current context can be defined as "tangible and intangible compensation" offered by organizations in return for employee whistleblowing of ISP violations. Examples include pay rises, bonuses, promotion, verbal appreciation, or positive assessment reports (Bulgurcu et al., 2010). In the whistleblowing literature, cognitive learning theory posits that employees learn regarding the effectiveness of whistleblowing from past experience (Lowry et al., 2013, p. 157). Therefore, if employees know that previous whistleblowers have been rewarded by organizational authorities, then their motivation to whistleblow increases (Lowry et al., 2013, p. 157). In practice, incentives are considered to be helpful to promote intended behaviors with regard to fostering a security culture within organizations (Eric and Goetz, 2007, p. 23). As one practitioner states in an interview "you have to reward people when they are doing security well, when they are practicing a safe computing environment" (Eric and Goetz, 2007, p. 23). Based on these arguments, we posit that rewards should encourage desirable security practices, including those that help management to uncover ISP violations. Thus, we hypothesize that

H4a: Extrinsic reward positively relates to individual gain of whistleblowing.

3.4.2. Intrinsic Benefits

Similarly, intrinsic benefits can be defined as internal positive feelings arising from personal achievement (Bulgurcu et al., 2010). Previous studies on whistleblowing (e.g., Miceli, 1992) have indicated that whistleblowers may personally gain from viewing the enactment of the professed standard since they would thereafter be entitled to behave according to their ideal moral values. This concept complies with the empirical findings of Bulgurcu et al. (2010), where internal reasons (or intrinsic motives) such as content, satisfaction, fulfillment and accomplishment are found to motivate employee compliance with ISP. Since complying with ISPs (i.e., merely obeying the rules) is a relatively more passive act compared with whistleblowing ISP violations, we believe that the induced personal achievements would be more eminent when employees proactively inform management of ISP violations. Thus, we hypothesize that

H4b: Intrinsic benefit positively relates to individual gain of whistleblowing.

3.4.3. Work Retaliation Victimization

Work retaliation victimization is defined as "adverse actions" intentionally taken against whistleblowers to alter their working conditions (Cortina and Magley, 2003). Examples include dismissal, unfair disciplinary actions, and poor performance evaluation (Cortina and Magley, 2003). These actions are generally initiated by those in the positions of authority such as supervisors and managers, and these actions often appear as tangible punishment that will be left on an employee's records (Cortina and Magley, 2003). Given that retaliation is the most commonly discussed inhibitor of whistleblowing activities, this study questions whether perceived risk of work retaliation impacts employees' attitudes toward whistleblowing ISP violations.

To establish this argument, we introduce a real-world whistleblower who was expeled after exposing internal security flaws. According to the online article titled "Data Security—Whistleblowing 101 for IT Professionals" published in 2008, the protagonist of the story[1] noticed some seriously inappropriate security practices within the organization. The protagonist decided to disclose the problems knowing that he would be the one to blame if the data breach were discovered. Unfortunately, this whistleblower was later called into the office and informed of the manager's decision to terminate his employment. This incident resulted in several discussions in the online community for IT professionals. Many also shared their thoughts regarding how to avoid retaliatory actions if IT workers determine to whistleblow security flaws. Therefore, based on this incident and several subsequent discussions, we argue that the fear of work retaliation could possibly serve as an employee's reason against whistleblowing ISP violations. In this regard, we propose the last hypothesis in this study as follows.

H4c: Work retaliation victimization negatively relates to individual gain of whistleblowing.

Ⅳ. Research Methodology

This study adopted the survey approach to test the proposed research model. Survey participants were restricted to those who work in an environment where ISP or any other guideline specifying acceptable and unacceptable uses of IT resources has been formally established. In the sections that follow, we explain our survey design and data collection procedures.

4.1. Construct Operationalization

The research constructs were operationalized using validated items from prior literature All research constructs except "positive consequence to employing organization" were reflective. Intention was measured using four items adapted from Park and Blenkinsopp (2009). Other reflective constructs were adapted from Bulgurcu et al. (2010) to fit the ISP whistleblowing context in this study. The measurement items for positive consequence to employing organization were adapted from Miceli and Near (1992). Positive consequence of whistleblowing to employing organization was specified as a formative construct because the consequences capture different dimensions of the core construct and removing any of them would alter the theoretical definition of positive consequence of whistleblowing to employing organization (see Petter et al., 2007). All measurement items used in this study were assessed using seven-point Likert scales from strongly disagree (or very

[1] The full media coverage can be found at https://whistlersear.wordpress.com/data-security-whistleblowing-101-for-it-professionals/.

unlikely) to strongly agree (or very likely)

This study included several control variables in the model (Bulgurcu et al., 2010). Individual-level control variables included gender, age, knowledge in computer and IT, tenure in current organization, and past whistleblowing experience, and organizational-level control variables included organization size (number of employees) and IT intensiveness (the extent to which the business operation depends on IT). Because the questionnaire was to be distributed in a Chinese context, we invited one professional translator and one professor specializing in information security policy to assist the translation of the instrument into Chinese to ensure that no loss of information was present.

Content validity was ensured by consulting three processors and one industry expert in the information security management domain. After several rounds of modification and clarification, only minor problems such as word order, expressions, term selection existed and had been fixed. Non-applicable items were either dropped or modified as suggested. We also recruited three industry experts from different backgrounds to further refine the measurement items and the online survey presentation to render it more understandable to the respondents.

Forty respondents participated in the pilot test. Analysis showed that all reflective measures possessed satisfactory reliability and validity. Although the formative measures failed to present acceptable measurement properties, we proceeded to the next stage because such failure might be the result of insufficient sample size in the pilot test.

4.2. Data Collection

The questionnaire was distributed through social networks and the biggest bulletin board system in Taiwan: PTT (telnet://ptt.cc). The former channel performed URL forwarding through Facebook, mobile instant messaging apps, and emails, and the latter contained discussion forums of various themes, allowing for a wider range of respondent population. Respondents were reminded that there were no right or wrong answers to the questions and that confidentiality would be guaranteed through anonymity.

Of the 275 responses we collected, 238 (86.6 percent) were from social networks and 37 (13.5 percent) from PTT. Responses were regarded invalid and thus excluded from data analysis if they failed to meet either of the two following criteria. First, respondents needed to work for an organization with an established ISP. Second, respondents needed to spend reasonable time (more than one minute) to complete all the questions in the survey. As a result, 24 out of 275 responses (8.7 percent) were deemed invalid, yielding a valid response rate of 91.3 percent. The profile of valid respondents is summarized in <Table 1> and <Table 2>.

Ⅴ. Data Analysis

This study used SmartPLS 2.0 for data analysis. The partial least squares (PLS) approach was employed because it can accommodate both formative and reflective constructs (Chin, 1998). Moreover, PLS is recommended for research models that are prediction-oriented and in the early stages of theory development (Fornell and Bookstein, 1982; Fornell and Cha, 1994). Because there exist little empirical research and prior theory on modeling the decision-making process of whistleblowing behavior toward information security policy violations, the current study is considered an advance in theory development. PLS is thus suitable for our research purposes.

<Table 1> Respondent Profile – Person

	Frequency	Percentage
Gender		
Male	125	49.80
Female	126	50.20
Age		
20 – 25	73	29.08
26 – 35	104	41.43
36 – 45	28	11.16
46 – 55	29	11.55
56 – 65	16	6.37
66 – 75	1	0.40
Education Level		
High School or below	7	2.79
College/Undergraduate	141	56.18
Masters	100	39.84
PhD	2	0.80
Other	1	0.40
Tenure in Current Organization (years)		
< 1	66	26.29
1 – 3	82	32.67
3 – 5	25	9.96
5 – 10	28	11.16
10 – 20	21	8.37
20 – 30	18	7.17
> 30	11	4.38
Respondent Knowledge of Computer and IT (Self-Assessment)		
Very Low	0	0.00
Low	2	0.80
Somewhat Low	6	2.39
Average	81	32.27
Somewhat High	53	21.12
High	74	29.48
Very High	35	13.94
Respondent Experience of Whistleblowing ISP Violation		
Yes	37	14.74
No	214	85.26

<Table 2> Respondent Profile – Employing Organization

	Frequency	Percentage
Industry		
Education	11	4.38
Financial Services	42	16.73
Government	19	7.57
Manufacturing	41	16.33
Non-Profit	4	1.59
Medical Services, Pharmacology, Biotechnology and Healthcare	10	3.98
Real Estate	1	0.40
Services	33	13.15
Information Technology	56	22.31
Telecommunications	5	1.99
Travel	3	1.20
Wholesale/Retail	5	1.99
Other	21	8.37
Organization Size (Number of Employees)		
Less than 500	97	38.65
500 – 999	21	8.37
1,000 – 4,999	70	27.89
5,000 – 10,000	21	8.37
More than 10,000	42	16.73
IT Intensiveness of the Organization (Self-Assessment)		
Not intensive at all	5	1.99
Not intensive	6	2.39
Not so intensive	9	3.59
Average	45	17.93
Somewhat intensive	37	14.74
Intensive	76	30.28
Highly intensive	73	29.08

5.1. Measurement Model

To ensure the instrument possessed acceptable measurement properties, we first examined the reliability, convergent validity, and discriminant validity of reflective constructs. We then assessed multicollinearity and indicator weights of positive consequence to the organization, the only formative construct in the research model. Finally, we examined the extent of common method bias to assess its impact to data analysis results.

<Table 3> shows the composite reliability and Cronbach's alpha values of the reflective constructs. All these values were above 0.8, exceeding the sug-

<Table 3> Composite Reliability, Cronbach's Alpha, and AVE

Reflective Constructs	Composite Reliability	Cronbach's Alpha	AVE
Intention	0.937	0.910	0.787
Attitude	0.946	0.924	0.815
Normative belief	0.891	0.818	0.732
Self-efficacy	0.961	0.940	0.892
Organizational gain	0.910	0.868	0.717
Individual gain	0.954	0.928	0.873
Extrinsic reward	0.934	0.906	0.780
Intrinsic benefit	0.959	0.943	0.855
Work retaliation victimization	0.982	0.980	0.889

gested threshold value of 0.7 (Hair et al., 1998; Nunnally, 1978). This result demonstrated high internal consistency among the reflective measures.

Convergent validity can be established if the average variance extracted (AVE) values are larger than 0.5 and all factor loadings are significant and above 0.5 (Fornell and Larcker, 1981). As shown in <Table 3> and <Tab1e 4>, the smallest AVE value was 0.717 (organizational gain) and the smallest factor loading was 0.817 (NORB1), thus ensuring acceptable convergent validity of the measures.

Furthermore, we assessed discriminant validity by examining whether an item's factor loading was higher than all of its cross loadings (Hair et al., 2011), and whether the square root of the AVE of each construct was higher than the correlations of that construct with the other constructs (Fornell and Larcker, 1981; Gefen and Straub, 2005). Satisfactory discriminant validity could thus be assured, as shown In <Table 4> and <Table 5>.

To examine the measurement properties of positive consequence to the organization, we followed Cenfetelli and Bassellier's (2009) suggestion to assess (1) whether the multicollinearity problem existed, and (2) whether the formative indicators possessed significant weights. High multicollinearity among formative indicators indicates undesirable conceptual overlap and may increase the instability of indicator weights (Cenfetelli and Bassellier, 2009). The largest variance inflation factor (VIF) value of the formative indicators was 2.425 (see <Table 6>), lower than the suggested threshold value of 5 (Hair et al., 2011). Therefore, multicollinearity was not a serious concern to this study.

A preliminary analysis of the formative indicators showed that most of the weights were non-significant. We thus followed Cenfetelli and Bassellier's (2009) guildelines on handling non-significant indicator weights by decomposing positive consequence of whistleblowing to employing organization into three sub-constructs, namely employee problem resolution, managerial resolution, and avoidance of accountability to external parties. Positive consequence of whistleblowing to employing organization was thus specified as a second-order construct consisting of the three sub-constructs that represent the positive outcomes of whistleblowing (see Jarvis et al., 2003). Further analysis, as shown in <Figure 2>, supported the re-specified structure, thus the formative construct of positive consequence of whistleblowing to

<Table 4> Factor Loadings

	INT	ATT	NORB	SEFF	ORGG	IDVG	EXTR	INTB	WRV
INT1	**0.927**	0.692	0.662	0.367	0.523	0.456	0.359	0.430	-0.082
INT2	**0.897**	0.667	0.597	0.421	0.523	0.403	0.309	0.405	-0.063
INT3	**0.855**	0.558	0.524	0.324	0.413	0.446	0.223	0.333	0.020
INT4	**0.867**	0.616	0.584	0.312	0.429	0.412	0.283	0.366	-0.100
ATT1	0.702	**0.885**	0.621	0.359	0.486	0.460	0.262	0.466	-0.067
ATT2	0.594	**0.889**	0.518	0.287	0.587	0.406	0.212	0.379	-0.123
ATT3	0.639	**0.925**	0.626	0.366	0.561	0.446	0.283	0.436	-0.128
ATT4	0.652	**0.913**	0.620	0.323	0.542	0.464	0.267	0.413	-0.154
NORB1	0.640	0.672	**0.817**	0.332	0.569	0.541	0.334	0.498	-0.016
NORB2	0.472	0.426	**0.825**	0.213	0.432	0.290	0.367	0.257	-0.048
NORB3	0.580	0.562	**0.921**	0.311	0.527	0.416	0.389	0.366	-0.030
SEFF1	0.361	0.347	0.335	**0.951**	0.292	0.211	0.137	0.253	-0.079
SEFF2	0.390	0.350	0.347	**0.950**	0.300	0.202	0.148	0.253	-0.145
SEFF3	0.390	0.352	0.285	**0.934**	0.239	0.204	0.172	0.228	-0.094
ORGG1	0.466	0.550	0.556	0.318	**0.821**	0.305	0.223	0.317	-0.166
ORGG2	0.485	0.499	0.546	0.271	**0.867**	0.374	0.306	0.322	-0.016
ORGG3	0.435	0.511	0.483	0.161	**0.857**	0.455	0.214	0.319	-0.036
ORGG4	0.423	0.472	0.449	0.235	**0.841**	0.444	0.252	0.284	0.024
IDVG1	0.450	0.507	0.523	0.268	0.480	**0.929**	0.483	0.559	0.014
IDVG2	0.479	0.472	0.475	0.164	0.442	**0.946**	0.490	0.578	0.055
IDVG3	0.425	0.400	0.406	0.178	0.376	**0.929**	0.574	0.542	0.119
EXTR1	0.345	0.239	0.363	0.142	0.290	0.551	**0.890**	0.512	0.145
EXTR2	0.283	0.293	0.408	0.119	0.270	0.479	**0.890**	0.553	0.073
EXTR3	0.272	0.219	0.354	0.163	0.207	0.418	**0.855**	0.481	0.031
EXTR4	0.273	0.252	0.372	0.151	0.260	0.485	**0.897**	0.513	0.135
INTB1	0.373	0.390	0.412	0.225	0.320	0.575	**0.555**	**0.944**	0.104
INTB2	0.390	0.398	0.407	0.231	0.301	0.561	0.512	**0.940**	0.080
INTB3	0.423	0.451	0.406	0.252	0.350	0.547	0.575	**0.934**	0.134
INTB4	0.426	0.504	0.445	0.253	0.395	0.530	0.515	**0.879**	0.094
WRV1	-0.049	-0.122	-0.050	-0.159	-0.054	0.042	0.088	0.092	**0.901**
WRV2	-0.056	-0.110	-0.019	-0.084	-0.016	0.058	0.125	0.139	**0.947**
WRV3	-0.067	-0.108	-0.018	-0.102	-0.060	0.044	0.113	0.130	**0.949**
WRV4	-0.036	-0.117	-0.014	-0.092	-0.049	0.104	0.127	0.114	**0.956**
WRV5	-0.101	-0.147	-0.077	-0.116	-0.136	0.042	0.079	0.076	**0.943**
WRV6	-0.090	-0.148	-0.062	-0.136	-0.094	0.041	0.082	0.057	**0.945**
WRV7	-0.076	-0.129	-0.027	-0.096	-0.035	0.057	0.100	0.100	**0.958**

Note: INT = intention; ATT = attitude; NORB = normative belief; SEFF = self-efficacy; ORGG = organizational gain; IDVG = individual gain; EXTR = extrinsic reward; INTB = intrinsic benefit; WRV = work retaliation victimization.

<Table 5> Correlation Matrix and AVE

	ATT	EXTR	IDVG	INT	INTB	NORB	ORGG	SEFF	WRV
ATT	**0.903**								
EXTR	0.284	**0.883**							
IDVG	0.492	0.552	**0.935**						
INT	0.717	0.335	0.483	**0.887**					
INTB	0.470	0.583	0.599	0.435	**0.925**				
NORB	0.662	0.424	0.501	0.670	0.451	**0.856**			
ORGG	0.602	0.293	0.463	0.536	0.368	0.604	**0.847**		
SEEF	0.370	0.162	0.218	0.403	0.259	0.341	0.293	**0.945**	
WRV	-0.131	0.113	0.067	-0.066	0.111	-0.035	-0.062	-0.113	**0.943**

Note: Diagonal items in bold are the square roots of the AVE. Off-diagonal items are the correlations between constructs.

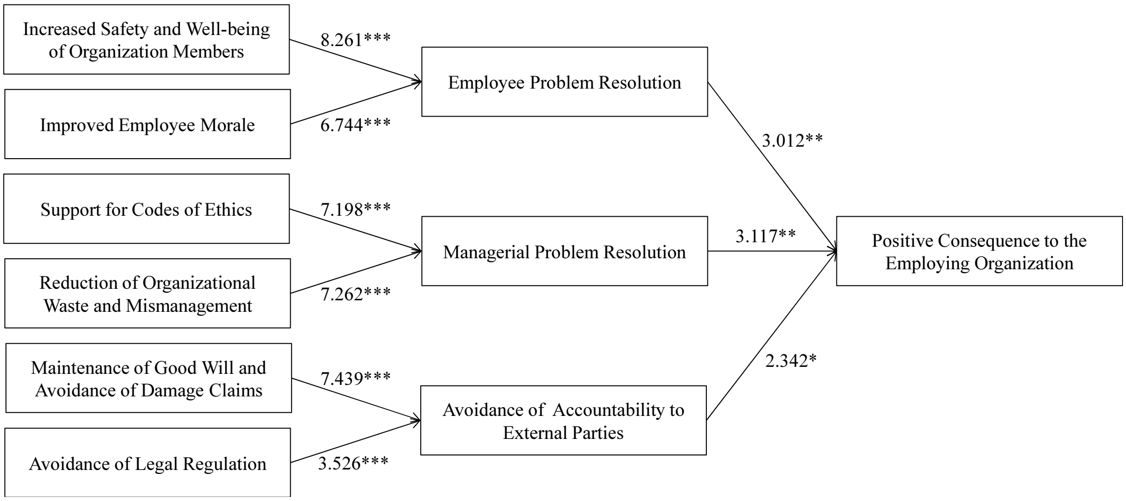
<Table 6> Multicollinearity Statistics

Dependent Variable: POSC1		Dependent Variable: POSC2		Dependent Variable: POSC3	
Independent Variables	VIF	Independent Variables	VIF	Independent Variables	VIF
POSC2	2.264	POSC3	1.563	POSC4	1.519
POSC3	1.765	POSC4	1.532	POSC5	1.342
POSC4	1.127	POSC5	1.193	POSC6	1.459
POSC5	1.347	POSC6	1.270	POSC1	1.849
POSC6	1.489	POSC1	1.761	POSC2	2.104
Dependent Variable: POSC4		Dependent Variable: POSC5		Dependent Variable: POSC6	
Independent Variables	VIF	Independent Variables	VIF	Independent Variables	VIF
POSC5	1.347	POSC6	1.493	POSC1	1.891
POSC6	1.467	POSC1	1.896	POSC2	2.072
POSC1	1.387	POSC2	2.16	POSC3	1.769
POSC2	2.425	POSC3	1.804	POSC4	1.513
POSC3	1.786	POSC4	1.54	POSC5	1.347

Note: POSC = positive consequence to the employing organization

employing organization was deemed valid.

To assess the degree of common method variance (CMV), we first performed Harmon's single factor test (Podsakoff et al., 2003). No single factor emerged that explained a majority of the covariance (the largest variance explained was 34.06 percent). Second, Pavlou et al. (2006) suggested that common method bias exists if correlations between research constructs are larger than 0.9. The highest correlation coefficient in <Table 5> is 0.717. The third approach we applied was the post-hoc marker-variable technique, which suggests that "the smallest correlation among the manifest variables provides a reasonable proxy for CMV" (Lindell and Whitney, 2001, p. 115). We


Increased Safety and Well-being of Organization Members
Improved Employee Morale
Support for Codes of Ethics
Reduction of Organizational Waste and Mismanagement
Maintenance of Good Will and Avoidance of Damage Claims
Avoidance of Legal Regulation
8.261***
6.744***
7.198***
7.262***
7.439***
3.526***
Employee Problem Resolution
Managerial Problem Resolution
Avoidance of Accountability to External Parties
3.012**
3.117**
2.342*
Positive Consequence to the Employing Organization

***: p<0.001; **: p<0.01; *: p<0.05. The values represent t-values.

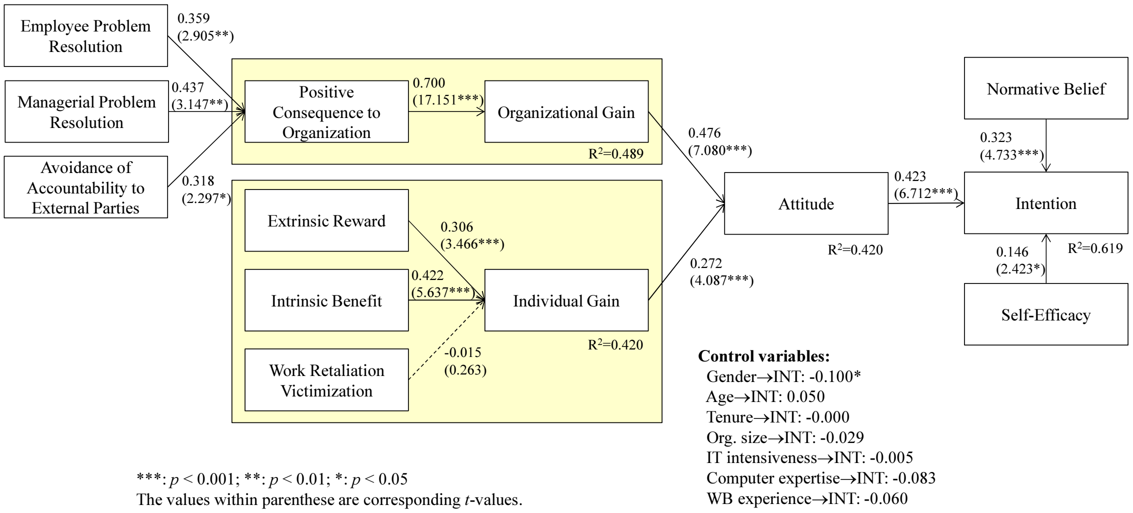
<Figure 2> Significance of Formative Indicator Weights (t-Values)

selected the seven items of work retaliation victimization as the marker variable because the average correlations with all other items was as low as 0.081. A new CMV-adjusted correlation matrix was then developed (Malhotra et al., 2006). We then followed the procedure suggested by D'Arcy et al. (2009) to examine the effect of CMV. The result revealed that all hypotheses were once again supported to nearly the same levels of significance, irrespective of the removal of CMV effects. The variance explained in intention (excluding the effect of control variables), attitude, organizational gain, and individual gain was 0.59, 0.45, 0.64, and 0.42, respectively. The evidence above showed that common method bias is not a major threat to the results of the current study.

5.2. Structural Model

A bootstrapping procedure with resamples of 600 was employed to test the significance of path coefficients. Overall, the model was supported and explained 61.9 percent of the variance in whistleblowing intention. The model demonstrated high explanatory power and provided support for all proposed hypotheses, with the exception of H4c.

The significant effects of attitude, normative belief, and self-efficacy on intention supported H1a (β = 0.423; p < 0.001), H1b (β = 0.323; p < 0.001), and H1c (β = 0.146; p < 0.05), respectively. Both organizational gain (β = 0.476; p < 0.001) and individual gain (β = 0.272; p < 0.001) were significantly and positively related to whistleblowng attitude, supporting H2a and H2b. The model explained 42.0 percent of the variance in attitude toward whistleblowing. Consistent with H3, positive consequence significantly contributes to organizational gain (β = 0.700; p < 0.001) and explains 48.9 percent of the variance. The positive effects of extrinsic reward and intrinsic benefit on individual gain supported H4a (β = 0.306; p < 0.001) and H4b (β = 0.422; p < 0.001). These two factors explained 42.0 percent of the variance in individual gain.



Control variables:
Gender→INT: -0.100*
Age→INT: 0.050
Tenure→INT: -0.000
Org. size→INT: -0.029
IT intensiveness→INT: -0.005
Computer expertise→INT: -0.083
WB experience→INT: -0.060

***: $p < 0.001$; **: $p < 0.01$; *: $p < 0.05$
The values within parenthese are corresponding t-values.

<Figure 3> Structural Model Analysis

The findings are summarized in <Figure 3>, which also shows the results for control variables. Only gender, had a significant influence on intention. Moreover, the explained variance in whistleblowing intention increased by approximately 2 percent when the control variables were added into the model. It is thus evident that the factors incorporated into the research model played more important roles than demographic variables in determining whistleblowing intention.

Ⅵ. Discussion and Implications

6.1. Discussion

Exploiting TPB and RCT, this study proposes a theoretical model involving both organizational and individual factors to explain whistleblowing intention and attitude in regard to ISP violations. Overall, most of the hypotheses in this study gain support from the empirical tests. To further understand the meaning of the structural model test results, we interpret them as follows.

Through a survey of 251 respondents, we discover that the three TPB constructs (attitude, normative belief, and self-efficacy) individually exhibit sizable effects on whistleblowing intention. Looking at it from the surface, we can state that the extent to which one approves of whistleblowing behavior, the perceived social pressure from other organization members, and the confidence in one's own ability to conquer the whistleblowing barriers all correlate with individual intention to disclose perceived ISP violations. Moreover, we also validate our argument that attitude indeed plays the most critical role in determining whistleblowing intention. Overall, TPB maintains its applicability of explaining whistleblowing intentions in the ISP compliance context. The results of our hypothesis testing are in line with those of previous empirical studies on general whistleblowing (e.g., MacNab and Worthley, 2008; Park and Blenkinsopp, 2009; Trongmateerut and Sweeney, 2013).

Returning to the antecedents of whistleblowing attitude, this study proposes that the development of a whistleblowing attitude entails an overall assessmet of outcomes at both the organizational and individual levels. Consistent with the study by Dozier and Miceli (1985) and several IT-related whistleblowing studies (e.g., Park et al., 2008; Lowry et al., 2013; Park and Keil, 2009) utilizing POB framework, our empirical findings confirm that whistleblowing of ISP violations is indeed a pro-social behavior that involves both altruistic and egoistic concerns. Moreover, we discover that organizational gain (p-value < 0.001; $\beta = 0.4757$) significantly influences attitude than individual gain (p-value < 0.01; $\beta = 0.2722$). We interpret this finding by stating that altruistic elements might play a more decisive role than egoistic elements for determining a whistleblowing attitude, at least in the IS security context.

At the organizational level, "positive consequence of whistleblowing to employing organization" is related to organizational gain. Based on the second-order formative construct operationalized in this study, we discover that employee problem resolution (employee well-being ensured and morale improved), managerial problem resolution (ISP *support* and waste/mismanagement *reduction*), and avoidance of accountability to external parties (goodwill maintenance, damage claims, and legal regulation avoidance) together determine the well-being of the entire organization. To the best of our knowledge, *this finding* not only lends the *first empirical support* to *the conceptual* statements from *Miceli and Near (1992)* but also shows the importance of these organization outcomes beliefs in establishing employees' whistleblowing attitudes.

At the individual level, both extrinsic reward and intrinsic benefit are found to contribute to individual gain from whistleblowing; therefore, these two benefit factors are relevant in the overall assessment of individual gain prior to employee whistleblowing. This finding also lends support to the arguments raised by Keil et al. (2010, p. 790) that in some cases, employees receive personal benefit ("direct rewards and intrinsic rewards") from whistleblowing. Moreover, the findings of Bulgurcu et al. (2010) reveal that employees are motivated to comply with ISPs by both external incentives and internal feelings. As an extension, this study contributes evidence that relatively more proactive responses, such as helping the management to detect ISP violations, can also be encouraged by these two positive factors at an individual level. To compare these two, we learn that intrinsic benefit exhibits a much stronger influence than extrinsic reward on the assessment of individual gain, indicating a greater significance level and path coefficient size. This, in our belief, indicates that positive feeling arising from successfully uncovering ISP violations is a more useful determinant to create advantages for employees. Finally, work retaliation victimization is not found to affect individual gain in any manner. We introduce a notion that was not highlighted in the previous sections to contemplate the reasoning behind this result in more depth.

In the literature, whistleblowing is categorized as either internal whistleblowing or external whistleblowing. The former refers to the disclosure of wrongdoings to the authorities within the organization, whereas the latter refers to the disclosure of wrongdoings to parties outside the organization. In general, employees who accidentally discover wrongdoings within the organization first resort to internal measures (Grant, 2002). Only when all the internal approaches have been exhausted and they still fail to instigate a correction will they consider reporting the incident to external parties (Grant, 2002). The rationale behind such a phenomenon is that external whistleblowing, in general, impacts the organization by exposing internal flaws to the public (Miceli and Near, 1988; Miethe and Rothschild, 1994, p. 342). Hence, organizations favor internal whistleblowing instead of external whistleblowing because the former enables them to effectively control the negative effects of "negative publicity." In this study, we confine our research scope to internal whistleblowing since we attempt to help organizations rectify a wrongdoing before it evolves into an irremediable disaster rather than expose internal problems directly to the public and expect them to recover.

We believe that work retaliation is more likely to occur to those who resort to external whistleblowing. Since external whistleblowing, in general, creates irreversible outcomes for organizations, it becomes reasonable for us think that organizations would have no reason to treat external whistleblowers well. Once again reviewing a news release[2] that supports the viewpoint of H4c, we discover that the story's protagonist—who fell victim to workplace retaliation—had first reported the "shabby" security practices to the management, but he was completely disregarded. Later, this person decided to post comments online but was soon traced and identified by the management. For reasons of disclosing internal confidential information, this whistleblower was fired immediately. Therefore, based on the aforementioned reason, we argue that work retaliation victimization is more likely to happen in the context of external whistleblowing rather than in the current context of internal whistleblowing.

6.2. Theoretical Contributions

This study contributes to the research and theory in the following three aspects. First, previous studies regarding user compliance with ISPs have overwhelmingly restricted their research focus on how employees utilize organizational IS resources. Some (e.g., D'Arcy et al., 2009; Siponen and Vance, 2010) studies have adopted the deterrence approach to dissuade organization members from behaving improperly, whereas others (Bulgurcu et al., 2010; e.g., Herath and Rao, 2009; Johnston and Warkentin, 2010; Hart and Cooke, 2012) have investigated the factors influencing employee motivation to protect organizational IS resources. Employees in either sense are treated more as objects or risks to be managed by those at the upper levels of the organizational hierarchy. However, as we have argued throughout this study, employees can play different roles in enhancing the effectiveness of information security management by calling attention to information security breaches within the workplace. From this perspective, our study serves as one of the first to understand general employees as part of the managerial team to ensure both user compliance and data safety. These findings improve our understanding of employee whistleblowing as an alternative approach to counter against insider abuse in the context of information security compliance.

Second, in regard to whistleblowing literature, we substantiate the effectiveness of whistleblowing in the IT context. As modern organizations depend more heavily on IT to perform operations, internal frauds are prone to be conducted through technological means. Whistleblowing mechanisms have indicated its value in preventing IT project failures; however, studies focusing on information system risks are still few. This study caters toward this trend and thereby addresses the gap on the intersection of information security management and whistleblowing.

[2] http://www.theregister.co.uk/2008/05/23/tjx_fires_whistleblower/

Finally, to the best of our knowledge, this is the first study to investigate whistleblowing motivation through the rational assessment of behavioral outcomes. In formulating our theoretical model, we nearly exhaust all the good and bad results of whistleblowing to employing organization as well as to individuals. Employee beliefs in these different outcomes build upon a strong theoretical foundation and are embedded in the information security context. Although it was an unsuccessful attempt to put all the outcome beliefs through empirical testing, we still verify that several factors, which, to our best knowledge, have never been tested so far, significantly affect employee motivation to uncover ISP violations. For future studies aimed at a better theoretical model of whistleblowing decisions, our model serves as a fairly easy-to-understand, parsimonious, yet powerful framework for them to map the decision-making process of whistleblowers.

6.3. Managerial Implications

Leveraging whistleblowing mechanisms, we believe practitioners can more effectively mitigate information security risks. Considering the increase in information-related fraud in the modern workplace, business organizations, albeit underprepared at the moment, should realize the truth that their best defense could be those who witness deviant behaviors and choose to speak up in a timely manner (Kroll, 2013). While security audits and discreet management are considered to be pivotal for fraud prevention, it is also acknowledged that when middle or top managers themselves are the culprits, whistleblowing becomes the key means to uncover unethical practices (Kroll, 2013). Considering these potentially threatening loopholes, this study calls more practical attention to whistleblowing as a complementary approach for current information security management. With well-established reporting channels, we believe that financial loss and other intangible harms arising from security breach would decrease accordingly.

Based on an improved understanding of the factors affecting whistleblower attitude and intention, security managers now can effectively promote internal whistleblowing. As attitude is found to influence whistleblowing intention the most, we suggest managers to place more effort in fostering positive employee attitudes toward internal whistleblowing. Specifically, the perceived organization and individual gain among employees should be carefully considered to establish more favorable views in regard to whistleblowing ISP violations. Therefore, when advertising the desirability and effectiveness of whistleblowing, security managers should analyze the pros and cons of internal whistleblowing for both the organization and individuals.

Although the importance of detecting and correcting insider abuse is rather evident in many industry reports, arguments of this type have mostly centered on preventing or avoiding substantial financial loss, damage to business reputation, and lengthy litigation procedures. In this study, we explicitly explain six positive consequences of whistleblowing ISP violations based on the study by Miceli and Near (1992). An elaboration on how these results could be achieved using whistleblowing mechanism in the information security context is helpful for various types of communication within organizations. For instance, it should become more realistic for practitioners to reach a consensus and therefore foster a moral ethical climate within the organization by articulating the desirable results in the six aspects (i.e., ensuring other members' well-being, improving employee morale, supporting ISP, reducing mismanagement and waste, maintaining goodwill, and avoiding damage claims and legal regulation) during the security workshop and awareness program. Besides, these outcome beliefs at the organizational level are also validated to contribute to individual attitude, indicating that altruistic concerns are indeed involved in the whistleblowing decision.

Egoistic concerns, such as beliefs in extrinsic reward and intrinsic benefit, are also validated to associate with individual attitude. As intrinsic benefit is found to significantly influence individual attitude, we suggest that more emphasis should be placed on the positive feelings (i.e., fulfillment, achievement, and satisfaction) conveyed to employees by explaining how past whistleblowers halted perceived wrongdoings and achieved moral satisfaction. Although this result might be of interest to theorists, its practical value might not be as promising as others.

Finally, when designing the interface of an online whistleblowing reporting system, it is suggested that besides anonymity features, the importance of whistleblowing should also be highlighted "through cues, prompts, and its displays" (Lowry et al., 2013, p. 178). Both organizational and individual outcome beliefs consolidated in this study can be applied for writing the descriptions so that managers could further persuade potential whistleblowers into actualizing their intention. Moreover, managers who seek to formulate an internal whistleblowing policy should also try to align organizational and individual interests to more or less stimulate employee willingness to report.

6.4. Limitations and Future Research Directions

Despite the constant attempt to minimize flaws throughout the whole research process, this study still has several limitations and thus provides further research opportunities.

To begin with, a scenario-based experiment might be a better alternative than the traditional survey for the following reasons. First, for sensitive issues such as ethical decision making, setting up a hypothetical situation (vignette) enables researchers to indirectly measure responses. Thus, respondents may thus feel less intimidated to express their true opinions since they would only need to answer whether they would do the same as the character in the scenario. In so doing, respondents would be less likely to answer questions in a socially desirable manner. Second, a scenario-based method would allow more details regarding the context to be given to the respondents. Therefore, respondents could better familiarize themselves with the situation and the problem. Furthermore, researchers could also reduce the likelihood of measurement error by preventing respondents from responding to a wide range of different scenarios. In sum, scenario-based experiments could be another option for future researchers. Despite the advantages of scenario-based experiments, it must be considered that the representativeness of selected scenarios is an important issue. As indicated by Stylianou et al. (2013), IT advances very quickly, and managing new types of IT malpractices is difficult for managers. Employees may encounter never-seen-before computer-related dilemmas in the near future. Whether selected scenarios could reflect the current progress of IT needs to be retrospectively addressed.

Second, analyzing attitude and intention may not be sufficient to understand the real whistleblower behaviors. Regardless of how motivated employees may be to conduct a certain behavior, there is always a chance that they end up doing nothing. While we acknowledge that there might be alternatives to gather behavioral data, such as government lists of whistleblowers and digital records in the online whistleblowing reporting system, problems still persist with these alternatives. For instance, government lists of whistleblowers are confined to employees who work in the public sector. Digital records in the online whistleblowing reporting system may also be confined to those who resort to virtual reporting channels. In general, the difficulty of collecting data from real whistleblowers imposes an inevitable limitation to studies on whistleblowing. To more or less solve this problem, this study finds 37 self-reported whistleblowers in the respondent profiles. This could be a useful data source for researchers to conduct additional analyses if the sample size is sufficiently large. While we recognize that "self-report" does not equate to "actual," there should be little reason for them to report dishonestly.

Third, all the survey respondents in this study are employees in Taiwanese organizations. In other words, cultural factors have not been hypothesized to generate differences in the effects of all factors on whistleblowing attitude and intention. The generalizability of our study results to other cultural contexts should be questioned and thus entails more research attention to bare the mystery of different mindsets of people from various cultural backgrounds. Furthermore, because organizational culture or climate affects employee behavior (Berry, 2004; Bock et al., 2005; Kaptein, 2011; Key, 1999), one other suggestion for future research is the influence of organizational culture. Employees exhibit behaviors that are reinforced by organizational culture. The ethical culture of an organization may encourage or discourage employees' whistleblowing intention (Key, 1999). Therefore, organizational culture may serve as an antecedent to extrinsic reward or a moderator on the relationship between extrinsic reward and individual gain. Moreover, organizational climate may also influence the effect of work retaliation victimization on individual gain. This study thus suggests future studies to further investigate the effects of organizational culture on whistleblowing behaviors.

Finally, the applicability of cost and benefit analysis to whistleblowing research might stir another long debate. Some scholars (e.g., Lowry et al., 2013) would argue that ethical decisions such as whistleblowing do not fit the rational choice framework because explicit benefit for individuals (if there is any) barely exists in most whistleblowing cases. While we can understand the underlying logic for this argument, we take a slightly different interpretation to the applicability of cost and benefit analysis in this study. In line with some studies (e.g., Chen et al., 2013) that have indicated monetary rewards along with other incentives to promote whistleblowing, we can see that some organizations indeed depend on employee reporting to detect fraud in practice. When formulating our theoretical model, we were interested if such benefit could possibly play a role in determining employee intention to whistleblow ISP violations. In the end, our empirical findings also turn out to support such a proposition. Considering such strong disagreement between these two countering positions, we suggest that future research collect data for both theories and critically test them.

Ⅶ. Conclusion

Considering increasing insider threat to modern organizations, it is essential for both academics and practitioners to contemplate countermeasures that can be applied to reinforce current information security management. We believe that whistleblowing, albeit a widely used mechanism for financial fraud detection, can serve as an alternative approach for security managers to mitigate information risks in the workplace. Through a comprehensive framework grounded upon TPB and RCT, numerous altruistic and egoistic factors are examined and found to affect employee attitude as well as intention to whistleblow information security breaches. From a theoretical perspective, our study serves as a good basis for future research to refine the conceptual modeling of employee whistleblowing motivation. Organization leaders can also derive some inspiration here to support their aspiration for whistleblowing policy formulation and internal whistleblowing promotion.

<References>

[1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

[2] Ajzen, I. (2011). Constructing a theory of planned behavior questionnaire. Unpublished manuscript, Retrieved from https://people.umass.edu/aizen/pdf/tpb.measurement.pdf, Accessed May 5, 2015.

[3] Berry, B. (2004). Organizational culture: A framework and strategies for facilitating employee whistleblowing. *Employee Responsibilities and Rights Journal, 16*(1), 1-11.

[4] Bock, G.-W., Zmud, R. W., Kim, Y.-G., and Lee, J.-N. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators, social-psychological forces, and organizational climate. *MIS Quarterly*, 87-111.

[5] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

[6] Cenfetelli, R. T., and Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly, 33*(4), 689-707.

[7] Chen, C. X., Nichol, J., and Zhou, F. H. (2013). The effect of financial incentive framing and descriptive norms on internal whistleblowing. AAA 2013 Management Accounting Section (MAS) Meeting Paper, Retrieved from http://ssrn.com/abstract=2132852, Accessed June 5, 2015.

[8] Chin, W. W. (1998). Ciommentary: Issues and opinion on structural equation modelling. *MIS Quarterly, 22*(1), 7-16.

[9] Cortina, L. M., and Magley, V. J. (2003). Raising voice, risking retaliation: Events following interpersonal mistreatment in the workplace. *Journal of Occupational Health Psychology, 8*(4), 247-265.

[10] D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

[11] Dozier, J. B., and Miceli, M. P. (1985). Potential predictors of whistle-blowing: A prosocial behavior perspective. *Academy of Management Review, 10*(4), 823-836.

[12] ERIC, M., and Goetz, E. (2007). Embedding information security into the organization. *IEEE Security and Privacy, 5*(3), 16-24.

[13] Fornell, C., and Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing research, 19*(4), 440-452.

[14] Fornell, C., and Cha, J. (1994). Partial least squares. *Advanced Methods of Marketing Research*, 407, 52-78.

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

[16] Gefen, D., and Straub, D. (2005). A practical guide to factorial validity using PLS-graph: tutorial and

annotated example. *Communications of the Association for Information Systems*, *16*(5), 91-109.

[17] Grant, C. (2002). Whistle blowers: Saints of secular culture. *Journal of Business Ethics, 39*(4), 391-399.

[18] Hair, J. F., Ringle, C. M., and Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139-152.

[19] Hair, J. F., Ronald, L.T., Rolph, E. A., William, B. (1998). *Multivariate Data Analysis*. Prentice Hall, Englewood Cliffs, NJ.

[20] Herath, T., and Rao, H. R. (2009). Encouraging information security behavior in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

[21] Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660.

[22] Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199-218.

[23] Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behavior: An empirical study. *MIS Quarterly, 34*(3), 549-566.

[24] Kaptein, M. (2011). From Inaction to External Whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing. *Journal of Business Ethics*, *98*(3), 513-530.

[25] Keil, M., Tiwana, A., Sainsbury, R., and Sneha, S. (2010). Toward a theory of whistleblowing intentions: A benefit to cost differential perspective. *Decision Sciences, 41*(4), 787-812.

[26] Key, S. (1999). Organizational ethical culture: Real or imagined? *Journal of Business Ethics*, 20(3), 217-225.

[27] Kroll (2013). 2013/2014 Global Fraud Report.

[28] Liao, C., Lin, H.-N., and Liu, Y.-P. (2010). Predicting the use of pirated software: A contingency model integrating perceived risk with the theory of planned behavior. *Journal of Business Ethics, 91*(2), 237-252.

[29] Lindell, M. K., and Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114-121.

[30] Lowry, P. B., Moody, G. D., Galletta, D. F., and Vance, A. (2013). The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems, 30*(1), 153-190.

[31] MacNab, B. R., and Worthley, R. (2008). Self-efficacy as an intrapersonal predictor for internal whistleblowing: A US and Canada examination. *Journal of Business Ethics, 79*(4), 407-421.

[32] Malhotra, N. K., Kim, S. S., and Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865-1883.

[33] McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*(1), 417-442.

[34] Miceli, M. P., and Near, J. P. (1988). Individual and situational correlates of whistle blowing. *Personnel Psychology, 41*(2), 267-281.

[35] Miceli, M. P., and Near, J. P. (1992). *Blowing the Whistle: The Organizational and Legal Implications for Companies and Employees*. Lexington Books, New York, N.Y..

[36] Miethe, T. D., and Rothschild, J. (1994). Whistleblowing and the control of organizational misconduct. *Sociological Inquiry, 64*(3), 322-347.

[37] Nunnally J. (1978). *Psychometric Theory*. McGraw-Hill, New York, NY.

[38] Oh, L.-B., and Teo, H.-H. (2010). To blow or not to blow: An experimental study on the intention to whistleblow on software piracy. *Journal of Organizational Computing and Electronic Commerce, 20*(4), 347-369.

[39] Park, C., Im, G., and Keil, M. (2008). Overcoming the mum effect in IT project reporting: Impacts of fault responsibility and time urgency. *Journal*

of the Association for Information Systems, 9(7), 409-431.

[40] Park, C., and Keil, M. (2009). Organizational silence and whistle blowing on IT projects: An integrated model. *Decision Sciences, 40*(4), 901-918.

[41] Park, H., and Blenkinsopp, J. (2009). Whistleblowing as planned behavior – A survey of South Korean police officers. *Journal of Business Ethics, 85*(4), 545-556.

[42] Paternoster, R., and Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25*(2), 103-127.

[43] Pavlou, P. A., Liang, H., and Xue, Y. (2006). Understanding and mitigating uncertainty in online environments: a principal-agent perspective. *MIS Quarterly, 31*(1), 105-136.

[44] Petter, S., Straub, D., and Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623-656.

[45] Pierson, J. K., Forcht, K. A., and Bauman, B. M. (2007). Whistleblowing: An ethical dilemma. *Australasian Journal of Information Systems*, *1*(1), 58-62.

[46] Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879.

[47] Scott, J. (2000). Rational choice theory. In G. Browning, A. Halcli, and F. Webster (Eds.), *Understanding Contemporary Society: Theories of the Present*, 126-138.

[48] Siponen, M., and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487.

[49] Smith, H. J., Keil, M., and Depledge, G. (2001). Keeping mum as the project goes under: Toward an explanatory model. *Journal of Management Information Systems, 18*(2), 189-228.

[50] Stylianou, A. C., Winter, S., Niu, Y., Giacalone, R. A., and Campbell, M. (2013). Understanding the behavioral intention to report unethical information technology practices: The role of machiavellianism, gender, and computer expertise. *Journal of Business Ethics, 117*(2), 333-343.

[51] Symantec. (2012). 駭客攻擊與人為疏失並列企業資料外洩主因.

[52] Tan, B. C., Smith, H. J., Keil, M., and Montealegre, R. (2003). Reporting bad news about software projects: Impact of organizational climate and information asymmetry in an individualistic and a collectivistic culture. *IEEE Transactions on Engineering Management*, *50*(1), 64-77.

[53] Trongmateerut, P., and Sweeney, J. T. (2013). The influence of subjective norms on whistle-blowing: A cross-cultural investigation. *Journal of Business Ethics, 112*(3), 437-451.

◆ About the Authors ◆

Wei, Liang-Cheng

Wei, Liang-Cheng (Patrick) now works at IBM Taiwan as an Application Consultant. He completed his Master's degree in the Department of Information Management at National Taiwan University. During his time at NTU, his research interest mainly lies in the field of information security and risk management. His work has been presented at the *Pacific Asia Conference on Information Systems*.

Carol Hsu

Carol Hsu is a Professor in the Department of Information Management at National Taiwan University. She holds a Ph.D. in information systems from the London School of Economics and Political Science. Her current research interests focus on the organizational and cultural issues related to security policy and technology implementation. Her work has been published in the *MIS Quarterly, Information Systems Research, European Journal of Information Systems, and Communications of the ACM.*

Kai Wang

Kai Wang is Associate Professor and Chairman of Department of Information Management at National University of Kaohsiung, Taiwan. He received the Ph.D. degree in Business Administration from National Central University, Taiwan. Kai Wang was Senior Industry Analyst and Research Manager at Market Intelligence Center, Institute for Information Industry. His research interests include online consumer behavior, mobile commerce, and innovation in business models. His work had been published in *Information Systems Journal, International Journal of Electronic Commerce, Information and Management, International Journal of Information Management*, and others.

Submitted: December 21, 2015; 1st Revision: February 24, 2016; Accepted: February 26, 2016