Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2014 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2014

EMPLOYEE INTENTION TO WHISTLEBLOW INFORMATION SECURITY POLICY VIOLATION

Liang-Cheng Wei
College of Management, National Taiwan University, r00725052@ntu.edu.tw

Carol Hsu
College of Management, National Taiwan University, carolhsu@ntu.edu.tw

EMPLOYEE INTENTION TO WHISTLEBLOW INFORMATION SECURITY POLICY VIOLATION

Liang-Cheng Wei, College of Management, National Taiwan University, Taipei, Taiwan, R.O.C., r00725052@ntu.edu.tw

Carol Hsu, College of Management, National Taiwan University, Taipei, Taiwan, R.O.C., carolhsu@ntu.edu.tw

Abstract

Insider abuse has always been a significant threat to information security management in organization. In order to address this issue, in this research we propose whistleblowing as another complementary measure to other existent approaches to strengthen the internal information security management. In particular, we focus on an investigation of employee intention to whistle-blow information security policy (ISP) violation. Drawing on the theory of planned behavior and rational choice theory, we develop a theoretical model to understand the factors at the organizational and individual levels that might influence whistleblowing attitude and whistleblowing intention. Through a survey-based empirical investigation, we anticipate the results to enhance our existing knowledge on management of insider abuse against information security policy within organizations.

Keywords: Information security policy violation, internal whistleblowing, behavioral issues of information security, theory of planned behavior, rational choice theory.

1 INTRODUCTION

Despite the increasing confidence of the worldwide CIOs in their information security management, industry reports show that the number of information security incidents is still on the rise (PricewaterhouseCoopers 2012). Over-optimistic attitudes and diminished budgets might have resulted in the problems of degraded programs and neglected risks (PricewaterhouseCoopers 2012). For instance, one company could lose up to 4 million dollars for one incidence of data breach and $156 for each compromised record on average (Ponemon Institute 2011). 61% of the surveyed customers stated that they would stop using products or services offered by organizations compromising their personal data (PricewaterhouseCoopers 2012). Therefore, it becomes clear that data breach on the whole would bring about huge financial losses as well as other intangible harms to the organizations.

Regarding the source of information beaches, Symantec (2012) report found that 40.6% of the data breaches were due to hacker attacks, while another 48.2% were caused by insider negligence, including "accidentally made public", "theft or loss", and "insider theft". This shows that insider problems sometimes can be more threatening than external attacks (Symantec 2012).

However, regulating employee behavior is never an easy job (Herath & Rao 2009). To address this issue, some organizations may implement surveillance techniques to monitor every action of information system end users. There are some problems associated with the surveillance approach. First, this course of action "is extremely costly and may not be even practically possible" (Herath & Rao 2009). Secondly, several wrongdoings are hard to be detected through monitoring mechanisms. Hence, in this research, we consider whistleblowing as the alternative information security management approach to complement and reinforce the current information security protection against insider security breaches.

Whistleblowing, by definition, is an act of revealing wrongdoings within an organization to the public or those in positions of authority. Organizations establishing such mechanism within the working environment typically encourage internal staffs to speak up and to inform on others' unethical practices. It has been commonly utilized to discover and rectify wrongdoings that would otherwise endanger organizations' operation. Typical forms of such mechanism are reporting channels that ensure the reported case would be appropriately addressed. In practice, whistleblowing is applied to detect several types of wrongdoings in organizational settings, but research activities regarding computer-related incidents have been few (Pierson et al. 2007).

In this research, we consider insider security breach as a form of employee wrongdoings. From this perspective, we formulate two research questions: 1) what are the factors influencing an employee's intention to whistle-blow a perceived information security policy (ISP) violation? 2) What is the relationship between an employee's attitude and whistleblowing behavior? To address these research questions, we propose a theoretical model based on theory of planned behaviour and rational choice theory. These two theoretical approaches allow us to model the decision making process of whistle-blowers. Furthermore, we have classified the evaluation of whistleblowing consequences both at the organizational and individual level. We believe that an integrative approach through the survey data collected from employees in a wide range firms can deepen our understanding of employee's decision-making process to whistleblow possible ISP violations in organizations. Findings from this research are expected to provide theoretical insights and practical implications that inspire the design and implementation of whistleblowing channel and program in the modern organizations.

The paper is organized as follow. In the next section, we review the existing literature on information security policy compliance and studies on IT-related whistleblowing. We then discuss our theoretical model, which is followed by the description of methodological approach. We conclude by presenting the expecting contribution of this research study.

2 LITERATURE REVIEW

2.1 Empirical Studies on Information Security Policy Compliance

As mentioned earlier, information security policy compliance has become an important concern in organizations. Within the IS security literature, a number of studies have attempted to understand the drivers affecting how organization members respond to information security policy. Building on the criminological school of thoughts, D'Arcy et al. (2009) consider IS misuse as form of a criminal act, and applied the general deterrence theory to examine the roles of "perceived certainty of sanction" and "perceived severity of sanction" in deterring employees from abusing IS resources. Utilizing the same theoretical approach, Siponen and Vance (2010) additionally incorporate "neutralizing techniques" to explain the psychological patterns immoral employees who may adopt to justify their wrongdoings. In other studies, Herath and Rao (2009) draw upon "principal agent paradigm" to model the relationship 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' intention to comply with rules can be explained. Bulgurcu et al. (2010) examine the roles of rationality-based beliefs and information security awareness contributing to organizational members' decision-making process prior to determining their ISP compliance intention. Johnston and Warkentin (2010) consider the 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 recommended approach. Finally, Hu et al. (2012) examine the preceding effects of "top management support" and "organizational culture" on the attitude, subjective norm and perceived behavioral control, and analyze how these constructs influence individual intentions to comply with information security policy.

While we consider that the previous studies have helped to enhance our understanding of IS security policy compliance, these studies all primarily focus on the determinants of end user behavior itself to obey or violate information security policy. But very few studies can be found discussing the role of employee whistleblowing intention in the information security protection. As elucidated earlier, there are times when cases of IS misuse are too difficult to discover or too expensive to monitor. Therefore, we propose that other than paying sole attention to information system user behavior, it might be useful to look into employee intention to whistleblow internal ISP violations. In the following section, we discuss the application of whistleblowing in IS research field.

2.2 Empirical Studies on IT-related Whistleblowing

Bad news reporting concerning IT projects has been one of the most frequent applications of whistleblowing to the information system studies. Several studies (e.g. Park et al. 2008; Park & Keil 2009; Smith et al. 2001; Tan et al. 2003) have devoted their efforts to the understanding of why some individuals choose to remain silent on the real status of an IT project while others choose to communicate the bad news upward the organizational hierarchy (Park & Keil 2009). From theoretical perspective, Keil et al. (2010) develop an integrative middle-range theory to illuminate 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, while costs mostly centre on the retaliation whistleblowers might suffer from other organizational members (Keil et al. 2010). In addition, Keil et al. (2010) align their arguments with Miceli and Near (1992) that before reaching a decision, whistleblowers would ponder on the alternative courses of action and balance relevant benefits and costs. To theorize these concepts, they develop a central mediation between several whistleblowing factors and the corresponding intention to explain how the benefit-to-cost differential links the two sides of constructs. Different from the work by Keitl et al. (2010), Oh and Teo (2010) examine the role of whistleblowing as a countermeasure against software piracy in organizations. Specifically, they adopt the behavioral reasoning theory (BRT), an extension of Ajzen's theory of planned behavior

(TPB), to model individuals' external whistleblowing intention to disclose software piracy. In their research, BRT is used instead of TPB mainly because the authors want to incorporate the motivational mechanisms whistleblowers rely upon when formulating their judgment and decision making. Their empirical findings show that "reason for" and "reason against" are both significant predictors of one's attitude and that global motives (attitude, subjective norm, and perceived behavioral control) are all significant predictors of one's intention to blow on software piracy. In addition, they found that one is more likely to externally report software piracy when he or she has a bad relationship with the organization as well as when the perceived level of legal protection is high. Recently, Stylianou et al. (2013) shift the whistleblowing research to the domain of IT malpractices. They posit that the inherently fast-changing characteristics of IT innovation have created difficulties for organizations to form a shared belief in what should be considered illegitimate IT practices within the organization. Besides, since the government legislation and the ethics codes that provide guidance for IT professionals often fail to reflect the current progress of IT, employees struggle when faced with computer-related ethical dilemma (Stylianou et al. 2013). Moreover, Stylianou et al. (2013) argue that people tend to hold different moral attitudes toward objects in physical world and in digital world. Thus, they state that frauds involving digital measures may induce a different response from individuals compared to those involving physical objects. Accordingly, they conduct a research to study how whistleblowers of IT malpractices may differ from those of other disciplines. By examining the interacting effects of gender, computer literacy (programming experience) and personal value of Machiavellianism, they discover that female workers are more likely to blow the whistle on "intellectual property infringement" and "privacy rights violation". On the other hand, computer literacy is not found to be significantly related to whistle-blowing intention. Finally, Machiavellianism has a significant moderating effect not only on the relationship between gender and whistleblowing intention but on the one between computer literacy and whistleblowing intention. In sum, their study is one of the first studies to illuminate the role of whistleblowing intention in the information security context.

More recently, Lowry et al. (2013) have analyzed the factors that would drive the employee to use whistleblowing reporting system. In their research, they have differentiated the differences between traditional means of whistleblowing (e.g. direct notification; telephone hotlines; post office boxes) and system-based whistleblowing. Moreover, trust, risk and anonymity are argued to manifest different characteristics when the report initiating itself involves the use of IT artifacts. By adopting a causal path grounded on the pro-social organizational behavior (POB) model from the mainstream whistleblowing literature, they suggest that "failure ought to be reported", "responsibility to report", and "willingness to report" are linked with a sequential order. Their empirical results of a scenario-based experiment show some interesting findings. First, perceived risk to organization and to self are both significant predictors of "failure ought to be reported" and "responsibility to report". Second, trust in both report-receiving parties and the reporting system is found to contribute to one's "willingness to report". Finally, "confidence in anonymity" is conceptualized into five formative dimensions and is found to mitigate perceived risk to self as well as to enhance the two forms of trust. Overall, this research provides some ground-breaking findings for IS scholars to further explore the use of online whistleblowing mechanisms in the future. We hope that our research findings can extend this area of knowledge to enhance our understanding of whistleblowing in the context of information security compliance.

To sum up, studies in the information security literature generally focus more on employee information security policy compliance rather than internal whistleblowing. Recent literature on IT-related whistleblowing has indicated its potential value in managing IT malpractices. In this paper, we attempt to address the research gap in these two fields by investigating employee intention to whistle-blow information security policy violations. To achieve this, we incorporate rationality-based belief to develop a more comprehensive framework that reflects benefit and cost factors resided in a whistleblowing decision. The next section elaborates more on the formulation of our model.

3 MODEL

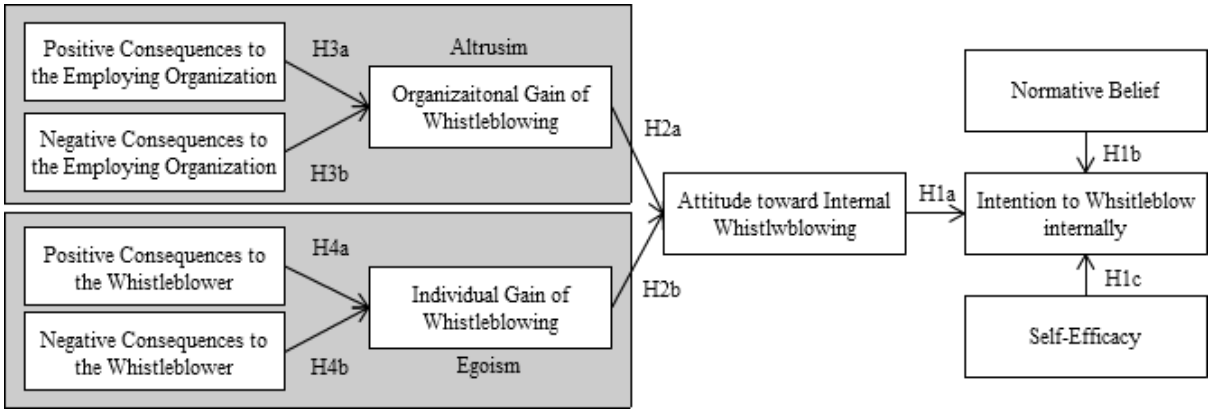

Figure 1. Research Model

To achieve the goal of explaining whistleblowing intention with a comprehensive framework, this study suggests using theory of planned behavior as a theoretical foundation. As is shown in the figure, an employee intention to internally report a perceived information security policy violation is influenced by attitude, normative beliefs (the antecedent of subjective norm), and self-efficacy (an equivalent concept to perceived behavioral control). Thus, in section 3.1, we introduce TPB and delineate how whistleblowing can be represented as a planned behavior. Next, in section 3.2, based on a brief introduction of rational choice theory, we propose that the decision making process of whistleblowers can be modelled by rational evaluation of all the likely consequences. Finally, in section 3.3, we differentiate these consequences into two levels and link them separately to the overall assessments of organizational and individual gains. Overall, four sets of hypotheses are presented in our theoretical model.

3.1 Theory of Planned Behavior

Theory of planned behavior, originally from Ajzen (1991), is one of the most powerful psychological frameworks used by researchers in various research fields to explicate the relationship between attitude, intention and behavior. Attitude refers to one's opinion about one behavior, while intention refers to one's 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 behavior in organizational environments is practically impossible or economically infeasible, scholars (e.g. Herath & 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 real whistleblowing behavior.

Three major determinants in this framework are believed to affect an individual's behavioral intention. Attitude refers to the degree to which one approves of one certain behavior. Subjective norm refers to the degree to which significant others agree with such planned behavior. Perceived behavioral control refers to the perceived ease of achieving that behavior. Numerous studies have shown that these three determinants account for a significant amount of variance in behavioral intention. Based on the essence of the utilized theoretical framework and the results of the previous empirical tests (e.g. MacNab & Worthley 2008; Park & Blenkinsopp 2009; Trongmateerut & Sweeney 2013) on whistleblowing intention, we hypothesize that:

- H1a: Attitude is positively related to the intention to internally whistle-blow information security policy violation.
- H1b: Normative belief is positively related to the intention to internally whistle-blow information security policy violation.
- H1c: Self-efficacy is positively related to the intention to internally whistle-blow information security policy violation.

Of all the three determinants presented above, attitude has shown to be relatively more important than the other two. Previous studies (e.g. Bulgurcu et al. 2010) have demonstrated that attitude is the only variable that can be externally manipulated by objective information. Besides, several derived theories (e.g. technology acceptance model) that originate from TPB also focus their attentions primarily on attitude. In this empirical investigation, we also attempt to understand the preceding factors determining the attitude of end user in the context of information security policy compliance. In theory of planned behavior, this factor is named behavioral belief. It is defined as an individual's subjective evaluation of each likely outcome that might follow the completion of the behavior (Ajzen 2011). Since 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 an interview with a representative sample of population to investigate the perceived advantages and disadvantages of the interested behavior so that a representative set of behavioral beliefs can be determined. In other words, people develop a positive or negative attitude toward one certain behavior based on their assessment of likely outcomes as either advantages or disadvantages to them. To further include this rationale, we introduce another framework to complement the current TPB model.

3.2 Rational Choice Theory

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). Drawing on the studies of Paternoster and Pogarsky (2009) and McCarthy (2002), Bulgurcu et al. (2010) proposed a procedure to explain how a person reaches a rational decision. They argue that decision makers at 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 outcomes (McCarthy 2002), each possible outcome of the certain behavior can be labelled 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 executing the certain behavior. After all the utility scores are derived, decision makers would compare the "good" of each alternative course of action and choose the one that maximizes their gain.

We believe that there is a linkage between TPB and RCT. In TPB, individuals foster their attitudes toward a behavior based on their subjective evaluation of likely outcomes, while in RCT, individuals assess the overall utility of outcomes for each alternative so that a decision can be made. Both of these two 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 TPB model coincides with many 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 possible outcome of whistleblowing as either a benefit or cost factor of individual attitudes.

Some studies (e.g. Lowry et al. 2013) may show their concerns toward the applicability of cost and benefit analysis to whistleblowing research. Scholars argue that explicit benefits for individuals could hardly be found (if there is any) in most whistleblowing cases. While we can understand the underlying thinking for this argument, in this research we take a slight different interpretation to the applicability of cost and benefit analysis. Some literature (e.g. Chen et al. 2013) has shown the support that monetary rewards along with other types of incentives are indeed used to encourage reporting fraud in practice. We are interested if such benefit could possibly play a role in determining employee intention to whistle-blow ISP violations. Furthermore, we consider that the term "benefit" refers to both explicit and intrinsic incentives. Studies (e.g. Bulgucu et al. 2010) have identified both

extrinsic and intrinsic benefit as factors of employee compliance with ISP. With this mind, we attempt to analyze whether active postures such as whistleblowing behaviours could be promoted by external incentives and internal positive feelings.

With respect to the dimensions involved in the evaluation of benefit and cost in whistleblowing, Dozier and Miceli (1985) argued that people balance benefits and costs into two levels. At the organizational level, a disclosure of wrongdoings may help the organization to recover from the wrongdoing itself, but it may also threaten the authority structures (Dozier & Miceli 1985). At the individual level, whistleblowers may suffer serious retaliation from other organizational members even though many of them think that what they did for the organization is morally acceptable.

In theorizing the benefit and cost at these two level, concerns over organizational gain are associated with altruism (an ethical disposition that intends for others' well-being regardless of the possible harm to the 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 it is more appropriate to discuss it from a pro-social perspective since the manner in which whistleblowers attempt to intervene and halt the perceived wrongdoings consists of both selfish and unselfish elements. Pro-social behavior, by definition, is a voluntary deed that attempts to help others in the society without ignoring self-interests and practical concerns. Therefore, we argue that there exists a spectrum manifesting the level to which the act of disclosing wrongdoings is out of altruistic motives or egoistic motives. By differentiating these two elements of whistleblowing behavior as the antecedents of individual attitudes, we believe interesting results might ensue and will guarantee an insight into the balance of altruism and egoism in whistleblower's minds. Thus, we hypothesize that:

- H2a: Organizational gain of whistleblowing is positively related to an individual attitude toward internal whistleblowing.
- H2b: Individual gain of whistleblowing is positively related to an individual attitude toward internal whistleblowing.

3.3 Altruistic and Egoistic Factors

To further develop altruistic and egoistic factors, at the organizational level, we draw upon the conceptual framework proposed by Miceli and Near (1992) to spread out all the favourable and unfavourable consequences of whistleblowing. Potential benefits 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", whereas potential costs to the employing organization include "challenge to authority structure", "threats to organizational viability", "limits on control", and "unpredictability of organization member actions" (Miceli & Near 1992). Each dimension of these two concepts can be put into the information security context and be given a new meaning. For example, given that corrective actions are taken following the whistleblowing report, we argue that information system resources of the organization would be safeguarded, the waste and mismanagement regarding IS resource 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. On the other hand, whistleblowing ISP violations might also challenge information security governance structure, threaten organizational viability (if the organization depends on that ISP violations to sustain its viability), limit others discretion to utilize IS resources, and increase the likelihood of others abusing whistleblowing mechanisms. Based on the above benefits and costs, we hypothesize that:

- H3a: Positive consequence to the employing organization is positively related to organizational gain of whistleblowing.
- H3b: Negative consequence to the employing organization is negatively related to organizational gain of whistleblowing

At the individual level, positive consequence to individuals can be twofold: extrinsic rewards and intrinsic benefits (Keil et al. 2010). Extrinsic reward can be defined as monetary or non-monetary incentives given by an organization to its employees in the hope of aligning the personal interest with the organizational one, whereas intrinsic benefit can be defined as positive feelings gained from personal achievement. The former is a widely-used approach to encourage certain actions within organizational environment, while the latter is said to be a very powerful incentive as internal motivation. We posit that both can be used to encourage whistleblowing of information security policy violations.

- H4a: Positive consequence to the individual is positively related to individual gain of whistleblowing.

Equally, there are negative consequences of whistleblowing at the individual level (Oh & Teo 2010). It can include retaliation against one's job-related duties and retaliation against one's interpersonal relationship (Cortina & Magley 2003). The former may appear in forms ranging from punitive transfer, demotion to dismissal, whereas the latter may appear in form of peer exclusion. We posit that both can discourage whistleblowing of information security policy violations.

- H4b: Negative consequence to the individual is negatively related to individual gain of whistleblowing.

4 EXPECTED CONTRIBUTION

In this research, our research objective is through empirical investigation, to examine the organization and individual factors that might influence the cognitive belief and assessment of whistleblowing of ISP violations in organization. In our next step of research, we plan to carry out an empirical investigation through survey method to collect data from employees in a variety of different organizations. We believe that there are two main theoretical and practical contributions of this research study. First, we will have an insight into what facilitates (or hampers) an employee intention to whistleblow wrongdoings in the information security context. Based on the results of this research, information security managers will be able to formulate relevant strategies that fully leverage this tool to counteract ISP violations. Specifically, a better understanding of the whistleblowing factors proposed in this study will offer practical suggestion for the design and implementation of whistleblowing mechanism to ensure information security policy compliance. Second, we contribute to the literature of whistleblowing by incorporating the concepts of rationality-based beliefs in TPB model. This allows us to develop a better analytical lens in examining the evaluation of benefits and costs associated with one particular behavior. Furthermore, our model highlights the importance to include such evaluation at both organizational and individual levels. Our study has some limitations. For instance, we decide to carry out the empirical test through the collection of survey data. People might have not actually take any action of whistleblowing before or be aware of possible whistleblowing opportunities in organizations. To address this, an alternative approach of using experiments with a different scenarios can further to test the evaluation of different considerations in employees' cognitive belief on whistleblowing intention. Second, it is possible that employees in different industries or in organizations of different operation scale might have different familiarity with the practices of whistleblowing. Future studies can either look into the possible variance in different industry sectors or group data by organizational size.

References

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Ajzen, I. (2011). Constructing a theory of planned behavior questionnaire. Unpublished manuscript. Retrieved, 1.

Bock, G.-W., Zmud, R. W., Kim, Y.-G., & 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.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS quarterly, 34(3).

Chen, C. X., Nichol, J., & Zhou, F. H. (2013, November). The Effect of Financial Incentive Framing and Descriptive Norms on Internal Whistleblowing. AAA.

Cortina, L. M., & Magley, V. J. (2003). Raising voice, risking retaliation: Events following interpersonal mistreatment in the workplace. Journal of occupational health psychology, 8(4), 247.

D'Arcy, J., Hovav, A., & 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.

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

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

Hu, Q., Dinev, T., Hart, P., & 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.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behavior: An Empirical Study. MIS quarterly, 34(3).

Keil, M., Tiwana, A., Sainsbury, R., & Sneha, S. (2010). Toward a Theory of Whistleblowing Intentions: A Benefit- to- Cost Differential Perspective*. Decision Sciences, 41(4), 787-812.

Liao, C., Lin, H.-N., & 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.

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

MacNab, B. R., & 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.

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

Miceli, M. P. (1992). Blowing the whistle: The organizational and legal implications for companies and employees: Lexington Books.

Oh, L.-B., & 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.

Park, C., Im, G., & 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).

Park, C., & Keil, M. (2009). Organizational Silence and Whistle- Blowing on IT Projects: An Integrated Model*. Decision Sciences, 40(4), 901-918.

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

Paternoster, R., & 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.

Pierson, J. K., Forcht, K. A., & Bauman, B. M. (2007). Whistleblowing: an ethical dilemma. Australasian Journal of Information Systems, 1(1).
Ponemon Institute. (2011). 2010 Annual Study: Global Cost of a Data Breach: Ponemon Institute.
PricewaterhouseCoopers. (2012). Changing the game: Key findings from The Global State of Information Security® Survey 2013.
Scott, J. (2000). Rational choice theory. Understanding contemporary society: Theories of the present, 126-138.
Siponen, M., & Vance, A. (2010). NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS. MIS quarterly, 34(3).
Smith, H. J., Keil, M., & Depledge, G. (2001). Keeping mum as the project goes under: Toward an explanatory model. Journal of Management Information Systems, 18(2), 189-228.
Stylianou, A. C., Winter, S., Niu, Y., Giacalone, R. A., & 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.
Symantec. (2012). 駭客攻擊與人為疏失並列企業資料外洩主因.
Tan, B. C., Smith, H. J., Keil, M., & Montealegre, R. (2003). Reporting bad news about software projects: Impact of organizational climate and information asymmetry in an individualistic and a collectivistic culture. Engineering Management, IEEE Transactions on, 50(1), 64-77.
Trongmateerut, P., & Sweeney, J. T. (2013). The influence of subjective norms on whistle-blowing: A cross-cultural investigation. Journal of business ethics, 112(3), 437-451.