2014 47th Hawaii International Conference on System Science

Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations

Miranda Kajtazi
Linnaeus University
miranda.kajtazi@lnu.se

Burcu Bulgurcu
Boston College
burcu.bulgurcu@bc.edu

Hasan Cavusoglu
University of British Columbia
cavusoglu@sauder.ubc.ca

Izak Benbasat
University of British Columbia
izak.benbasat@sauder.ubc.ca

Abstract

It has been widely known that employees pose insider threats to the information and technology resources of an organization. In this paper, we develop a model to explain insiders' intentional violation of the requirements of an information security policy. We propose sunk cost as a mediating factor. We test our research model on data collected from three information-intensive organizations in banking and pharmaceutical industries (n=502). Our results show that sunk cost acts as a mediator between the proposed antecedents of sunk cost (i.e., completion effect and goal incongruency) and intentions to violate the ISP. We discuss the implications of our results for developing theory and for re-designing current security agendas that could help improve compliance behavior in the future.

1. Introduction

Security practitioners in organizations typically intend to make employees acutely aware of information security problems [1, 2]. Employees, however, seem to establish their own practices and rationale for how they handle security rules and regulations of their organization. Growing evidence shows that information security plays an essential role for maintaining organization's good image, by enhancing it with a security-aware culture [3] or a general security climate [4], by counteracting employees' use of neutralization techniques [5], or by enforcing compliance with information security policies [6]. Yet, organizations appear ill-equipped to manage a healthy security culture.

Recent studies suggest that security practitioners need to shift their efforts towards ensuring that employees recognize information security threats and the risks these threats pose to their organization [7, 8]. As a consequence, employees have become widely known for their role as insider threats, causing most of the security breaches every year [9]. One of the biggest concerns for security practitioners is the insider threat [8, 9]. In their latest press release, the Information Security Forum informs us that the biggest risks in organizations stem from the increasing sophistication of known threats as they mature. In a recent study, Willison and Warkentin [8] state that "insiders are employees or others who have (1) access privileges and (2) intimate knowledge of internal organizational processes that may allow them to exploit weaknesses".

While security practitioners attempt to design new strategies towards securing information as their most invaluable organizational asset, they are rather uncertain whether to emphasize the technical or the behavioral issues related to information security [10]. As insider attacks mature, security practitioners still are indecisive whether increasing investments in specific security technologies, [11], or advancing their current information security strategy [10] is the best defense strategy against insider threats. For the former, according to traditional strategic approaches [12], organizations pick technologies based on their types of performances. Banks as well as pharmaceuticals or engineering companies, for instance, would like to achieve high security and reliability, [3, 13]. As for the latter, to take a decision on what is the most reasonable information security strategy for organizations is definitely a dilemma.

In organizations, emphasizing investments on security technologies has become the norm. Research informs us that secured channels should no longer be driven by security technologies alone, but also by controlling employees' misbehavior [3, 4, 5, 6, 8]. The objective of this paper is to develop a model that examines sunk cost factor as a mediating mechanism by testing its role to explain insiders' intentional violation of information security policy.

Although research in this area has tackled behavioral and organizational problems of this nature [3, 5, 6, 9, 13, 14], we have little understanding of it. Despite the growing research on noncompliance behavior with ISPs, studies suggest that information

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.393

security research is still in the process of forming a tradition where specific research foci are well-established and sufficiently investigated [7]. We believe that furthering the current understanding on employees' intentional violation of ISPs, both in terms of utilized theoretical lenses and empirical research is necessary for two reasons. First, the security of information in organizations continues to be one of the most serious issues [8, 15, 16], in particular that sophisticated insider threats are on the rise, exhibiting a challenging dilemma for organizations. Second, there are relatively few studies that focus on employees' violation of ISPs, when such behavior is committed intentionally because of employees' personal/ organizational reasons to do so [17].

The rest of the paper is structured as follows. We first introduce our theoretical framework in which the research model and the hypotheses are specified. We then present our research methodology, followed by data analyses and results. Finally, we draw a discussion on our findings, by presenting the limitations of this study, as well as its implications for theory and practice.

2. Theoretical framework

Violation involves a variety of behavioral activities. Despite the efforts organizations put to enforce their employees to comply with ISPs, employees often feel pressured to complete their projects at any cost, which suggest that ISPs become an impediment [3]. Employees' misuse of organizational resources, commonly leading towards intentional violation of the ISP, can originate in many situations. For instance, when an employee finds out that he/she cannot complete a project on his/her own, thus requires the help of an inside or outside expert, is determined to violate the ISP, rather than withdraw from the project and accept the loss. In this paper we develop a theoretical framework for addressing such situations. We draw on escalation of commitment theories [18] to explain how escalation factors affect intentional violation of ISPs. Theories of escalation of commitment explain the reasons why employees often become overly committed to failing courses of actions (e.g. when an employee is aware that his/her task is not progressing, and results in a nonperforming task); nevertheless persist on continuing [19]. The familiar escalation behavior, as perceived by researchers on project management [20, 21], may also explain employees' intentional violation of the ISP. Escalation theories intend to explain escalation of commitment behavior by focusing on factors that are commonly used to turn around a failing course of action; such as, investing more resources even if a project is failing, withholding project-related information from the management just to save personal image, or focusing on personal payoffs if the project meets the requirements and is accomplished. In this study we propose intentional violation of the ISP as an escalation behavior.

We attempt to explain it by using three escalation theories: (1) *Prospect Theory* to measure how the factor of sunk cost may be associated with insider's intentional violation of ISP; (2) *Approach Avoidance Theory* to measure how the factor of completion effect indirectly influences insider's intentional violation of ISP; (3) *Agency Theory* to test if goal incongruency indirectly influences insider's intentional violation of ISP.

Escalation behavior factors can potentially be utilized to extend the knowledge about insiders' intentional violation of ISP. We argue that the presented theoretical framework based on three selected factors, namely sunk cost, completion effect and goal incongruency, can help us predict a large proportion of variance to explain insider's intentional violation of the ISP. In doing so, we test our theoretical framework focusing on information – intensive organizations, such as banks and pharmaceutical industries that are known to be more vulnerable in protecting their information [3], than other types of organizations.

Table 1 presents these three factors that we utilize to design our theoretical framework. The table also intends to compare these factors by highlighting how each factor is utilized to explain intentional violation of ISP.

Table 1. Three escalation theories to explain intentional violation of ISP

Theory	Intentional Violation	Key Factors
Prospect Theory (PT)	Insiders would intentionally violate the ISP of their organization, because when they decide to commit more resources to a nonperforming task, they would rather choose to share classified information with experts in the field, just to get their help in completing the task which is failing, rather than	**Sunk Cost** invokes a choice between losses. Insiders would commit more resources (time, effort and money) to a failing course of action, e.g. a task at work, just to make sure they don't have to withdraw from the task, and as

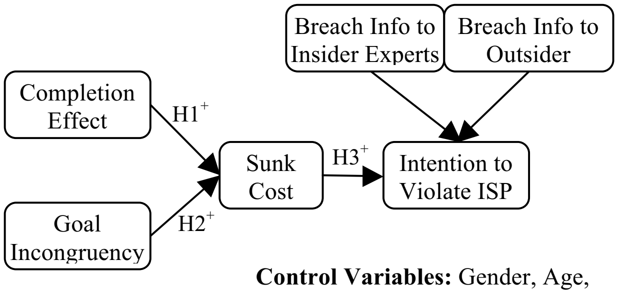
	withdraw from the task and accept the loss.	a result accept the loss.
Approach Avoidance Theory (AAT)	Insiders' intentions to reach the goal in completing their tasks at work, forces them to intentionally violate the ISP by sharing classified information with experts in the field, just to get their help in reaching the goal of completing the task.	**Completion Effect** known as proximity to the goal, is one of the key driving forces that pushes an insider towards escalation of commitment.
Agency Theory (AT)	Insiders decide to ask for the help of an expert by sharing classified information with them, because it is in their best interest to do so.	**Goal Incongruency** presents a condition in which an insider decides to act for their own benefit rather than the benefit of his/her organization.

We return to these factors in more details when we discuss our research model and develop the hypotheses in the subsequent section.

2.1. Research model and hypotheses

The research model formulation begins by adopting factors from escalation of commitment theories that serve as its predictors. Three escalation theories are central to understanding our depend factor of intentions to violate the ISP, which reflects employees' intentions to breach information to insider and outsider experts for personal benefits. We focus on prospect theory, in particular the sunk cost factor that acts as a mediating factor; approach avoidance theory, in particular the completion effect that acts as an independent factor; and, agency theory, in particular goal incongruency that also acts as an independent factor. The framework proposes that the violation of the ISP in escalation situations can be explained in terms of these three escalation factors. Figure 1 presents our research model.

The model posits that intentions to violation the ISP, occurs when insiders choose to ask for the help of an expert (insider or outsider) by sharing classified information with them, just to make sure that the project does not fail after a large amount of time, effort and money was invested.



Control Variables: Gender, Age, Education, IT Knowledge, IT Usage

Figure 1. Research model

More specifically, the model explains that employees would perceive their sunk costs, and that employees would then violate the ISP in trying to recover from the situation.

In our theoretical framework, approach avoidance theory suggests that the completion effect is a type of motivation for an employee to achieve a certain goal, particularly when the employee gets closer to that goal. The factor of completion effect may explain that when projects are near completion, insiders' intentions to violate the ISP increase, since their motivation to complete the project also increases. This leads us to the first hypothesis:

H1: Completion effect will positively influence insider's perception of sunk costs in their project.

According to agency theory, goal incongruency defines the agency as a problem. We consider this problem to be specifically related to the conflicting goals of security managers and employees in organizations. Employees often tend to take advantage of uncontrolled situations, particularly when they are able to act without being noticed by others. Employees, who are goal incongruent, will most likely act on the basis of their self-interest [19]. Therefore we formulate our second hypothesis, as follows:

H2: Goal incongruency will positively influence insider's perception of their sunk costs in their project.

Prospect theory, explains that an insider's intention to violate the ISP depends on the effect of sunk cost. Prospect theory suggests that employees who intentionally misbehave in regard to security practices in their organizations, most likely have not come to experience a punishment or a sanction, thus are more inclined to engage in risk-seeking behavior [22]. This phenomenon is commonly referred to as the sunk cost, which relates to at least three types of investments: sunk time, sunk effort and sunk money [18]. Therefore, we state the following hypothesis:

H3: Perceived sunk costs will positively influence insider's intention to violate the ISP.

To test the proposed model, we have conducted an empirical study. The research methodology is explained in the following section.

3. Research methodology

The empirical investigation relies on hypothetical scenario-based survey approach [5, 6, 7]. The survey instrument measures were created following the definitions and theory as well as the previously utilized survey instruments that study noncompliance behavior with ISPs [23]. The dependent variable—"Intention to Violate ISP"—was created as a formative second-order construct based on insiders' intentions to breach information to insider experts or to outsider experts.

The initial developed survey was first tested for content validity, construct validity and reliability [24, 25]. The validation procedure of our empirical study is based upon several rigorous steps taken before the survey was ready for the main study. In the first step, we initiated the instrument design by contacting several security experts and academics in the field. In total, we had feedback from twelve respondents (security experts and academics in the field), who were part of seven different organizations. Their feedback was crucial to test our initial proposed theoretical framework as well as to start validating the proposed instrument. We kept contacts with these respondents until a level of agreement was reached for the proposed survey.

The second step was a closed card-sorting exercise [26] with five participants (two professionals, two students and one academic) from two different organizations. The results concerning the three constructs in our research model showed that these constructs are distinct from one another and did not require merging or deletion. The participants, however, suggested that the items should be made clearer for a wider audience.

The survey was fine-tuned once again to facilitate its understanding by a wider audience as suggested by the academics, industry experts and the closed-cart sorting participants. The third step was then initiated. We had a pre-test where we initiated the distribution of the survey to selected faculty members and graduate students at an academic institution. Based on the pretest, we received a total of 31 valid responses, some by also commenting on the wording and length of the questions. These responses were both used for quantitative analysis for initial validity and reliability checks, and qualitative analysis for improving the appearance of the survey.

We then continued with the forth step to test our research model based on the exploratory factor analysis. We conducted a pilot study at the pharmaceutical industry. We received 20% (n=126) responses of the targeted group. Using exploratory factor analysis, the initial research model and some measurement items needed slight modifications. After the pilot study was complete and resulted in a stable model for further tests, we continued with the main study.

Our main study focused on the banking and pharmaceutical industry. The survey was distributed online via a web address provided by the home university, and remained active for a few days, due to strict security regulations imposed by the bank and the pharmaceutical companies. We designed the survey in the way that the identity of the participants was kept anonymous, and all participants responded to the survey on voluntary basis. Among the 1,556 contacted employees, approximately, 32.2% (n=502) responded to the survey. All participants were first presented a number of demographic questions, followed by a scenario. All responses were considered reliable and there were no missing answers.

4. Data analyses and results

We used the component-based partial least squares (PLS) approach to structural equation modeling (SEM) to test the measurement model and the structural model. The PLS, as a component based approach, is preferred over the covariance based approach because it is deemed adequate for exploratory models and theory development and is also considered to be more appropriate when formative indicators as well as reflective indicators are used to measure latent constructs within a research model [27]. We used the Smart-PLS software package (version 2.0.M3) to evaluate the psychometric properties of measurement scales and to test the research hypotheses.

4.1. Validity and reliability of measurements

We assessed the validity of the reflective constructs by examining their convergent validity, individual item reliability, composite reliability, and discriminant validity. The measures of all constructs have adequate reliability and validity assessments, thus, all were kept for structural model testing.

As reported in Table 4, The Average Variance Extracted (AVE) values for all reflective constructs are greater than the minimum recommended value of 0.50, thus convergent validity is ensured. Also, the square root of AVE for each reflective construct in the model is larger than the corresponding off-diagonal correlations of the construct to their latent variables, thus discriminant validity is ensured. The composite reliability values for the reflective constructs in the research model are greater than 0.87 and Cronbach's alpha values are greater than 0.78, demonstrating that all reflective constructs have adequate reliability assessment scores, ensuring scale reliability [23]. As reported in Table 3, all the measurement item loadings on respective constructs are above recommended minimum value of 0.707, indicating that at least 50 percent of the variance was shared with the construct, ensuring convergent validity [27]. Finally, all the measurement item loadings on the intended constructs are above 0.78 and at least 0.1 less on its loadings on other constructs, ensuring discriminant validity of the constructs. Table 5 presents the constructs and their measurement items, their mean, standard deviation and loadings, while Table 6 presents the survey instrument.

4.2. Structural model testing

We used the PLS approach to structural equation modeling and the bootstrapping resampling method for structural model testing. The results of the model estimation including standardized path coefficients, significance of the paths based on one-tailed t-test and the amount of variances explained (R^2) are presented in Figure 2.

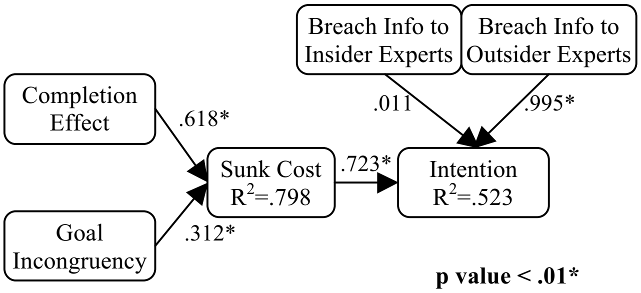


Figure 2. Structural model testing

The t and p values are reported in Table 2. As reported in Table 2, all of the three proposed hypotheses were supported at minimum of p<0.01.

Completion Effect and Goal Incongruency have a significant positive impact on Sunk Cost, predicting approximately 80% of the variance. Thus, hypotheses 1 and 2 are supported. Sunk Cost, in turn, has a significant positive impact on an employee's intention to violate the ISP, explaining approximately 52% of the variance. Thus hypothesis 3 is also supported.

Table 2. Hypotheses and t-values

	t - values	Supported (one-tail)	p-value
H1	8.39	√	p < .01
H2	4.34	√	p < .01
H3	20.84	√	p < .01
Insider → Intention	0.34	Not Supported	p < .15
Outsider → Intention	39.86	√	p < . 01

Breaching information to outsider experts – one of the proposed sub-constructs of the dependent variable – is found to be also highly significant in explaining Insider's Intention to Violate an ISP. However, breaching information to insider experts – the other proposed sub-construct of the dependent variable – does not significantly contribute to the underlying factor.

4.3. Discussions and implications

This study highlights the importance of an employee's perceived sunk cost as a determinant of his/her intention to violate the requirements of his/her organization's ISP, as it explains more than 50% of the variance in the dependent variable. Our results also suggest that an employee's perceived sunk cost can be predicted by completion effect and goal incongruency.

We suggested two sub-constructs for intention to violate the ISP: breaching information to insider experts and outsider experts. We found that breaching information to outsider experts significantly contribute to the underlying factor; however, breaching information to insider experts does not. We believe that this is an important finding, showing that employees are likely to disclose information to outsiders rather than insiders when they are in need of help to complete their job related tasks. While this situation may make it less likely for an employee to get caught as a result of his security breach, it may also make it more dangerous since information would be disclosed outside of their organization.

As organizations strive to get their employees to follow their information security rules and regulations, we believe that this study is important in emphasizing factors that precede an employee's information security breach. As an important practical implication of our results, organizations should develop a culture that employees are likely to perceive that complying with the security requirements would not feel costly or would not conflict with their job related tasks. Also, the results of this study show that employees are likely to consult with outsider experts to complete their job related tasks. To prevent this situation happening, it is important that employees feel the need to consult the insider experts rather than the outsider experts to complete their tasks without violating their organization's ISP. We suggest that organizations should be more careful in controlling the escalation of commitment behavior; however, this is not an easy task. Our results show that employees would typically breach classified information to outsider experts in order to receive the needed help, just to make sure they complete their tasks. We suggest that successful management of information security policies in organizations depends on reinforcement methods, requires better security awareness education and training, leading towards a healthy security culture. We recommend that security managers must encourage their employees to show honest and open project reporting in their organizations and they should also be able to assist their employees in finding insider experts to get the needed help.

5. Conclusions and future research

In this paper, we proposed a theoretical framework based on escalation of commitment theories to study insiders' intentions to violate organization's ISP. Three escalation theories were utilized, namely: prospect theory from which we adapt the factor of sunk cost; approach avoidance theory form which we adapt the factor of completion effect; and, agency theory from which we adapt the factor of goal incongruency. We utilized the escalation of commitment literature to problematize that insiders' intentions to violate the ISP is a result of their personal benefits to do so, which we tested based on these three escalation factors.

On the basis of the proposed theoretical framework, we developed a research model, which posits that insiders in organizations tend to violate the ISP when they breach information to insider and/or outsider experts for personal benefits. Empirically we tested our model by focusing on three different situations. First, we proposed that insiders would intentionally violate the ISP of their organization, because when they decide to commit more resources to a nonperforming task, they would rather choose to share classified information with experts in the field, just to get their help in completing the task which is failing, rather than withdraw from the task and accept the loss. Second, we proposed that insiders' intentions to reach the goal in completing their tasks at work, forces them to intentionally violate the ISP by sharing classified information with experts in the field, just to get their help in reaching the goal of completing the task. Third, we proposed that insiders decide to ask for the help of an expert by sharing classified information with them, because it is in their best interest to do so.

In all three situations we found empirical support by testing the proposed research model, based on the data from three information-intensive organizations. By testing our dependent variable as a formative second-order construct based on insiders' intentions to breach information to insider experts or to outsider experts, our empirical tests showed that employees would typically contact the outsider experts rather than the insider experts. This result indicated that employees tend to hide troubled task reporting, therefore they would rather contact the outsider experts who have no connection to their organization. If employees would choose to contact the insider experts, as a result, contacting them would result in disclosing the troubled tasks to the management. This is typically not beneficial for the employee, but for the organization. Testing the factor of goal incongruency proved that employees act for their interests rather than the interest of their organization.

Future research can look at identifying the other dimensions of ISP violation and test whether they significantly contribute to the overall factor. This could be an important research particularly for practitioners, since they can use those factors to formulate their ISP documents. Another fruitful future research direction could be to investigate whether an employee's active participation in the development and/or revision of the ISP document could play a role in shaping his/her perceived sunk cost. Understanding the goals and objectives of the specified rules and regulations in an ISP document can help perceive those rules less costly.

This study is also constrained by some limitations. The selection of participants may be one of the possible limitations of this study since the data represent only two industries. However, since these two industries are highly sensitive to information security breaches, they represent some of the most vulnerable types of organizations in regard to information security. Other types of industries may require adding other sets of constructs to conduct analyses on noncompliance behavior. Another limitation relates to the construct of completion effect. In utilizing this construct, instead of stating that the "task is near completion", our instrument can be advanced by being more specific that the "task is 50% completed, 75% completed or 99% completed". We believe that such specificity can generate interesting results for understanding whether employees would be less likely to comply with ISPs when for instance the task is 99% completed rather than 50%.

10. References

[1] Cone, B., C. Irvine, M.F. Thompson, and T.D. Nguyen, "A Video Game for Cyber Security Training and Awareness", Computers and Security, 26(1), 2006, pp. 63 - 72.

[2] Puhakainen, P. and M. Siponen, "Improving employees' compliance through information systems security training: an action research study", MIS Quarterly, 34(4), 2010, pp. 757-778.

[3] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awarenss", MIS Quarterly, 34(3), 2010, pp. 523-548.

[4] Herath, T. and H.R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations", European Journal of Information Systems, 18 (2), 2009, pp. 106-125.

[5] Siponen, M., and A. Vance, "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations", MIS Quarterly, 34 (3), 2010, pp 487-502.

[6] D'Arcy, J., A. Hovav, and D.F. Galleta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", Information Systems Research, 20 (1), 2008, pp. 79–98.

[7] Vance, A., and M. Siponen, "IS Security Policy Violations: A Rational Choice Perspective", Journal of Organizational and End User Computing, 24 (1), 2012, pp. 21-41.

[8] Willison, R. and M. Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse", MIS Quarterly, 37(1), 2013, pp. 1-20.

[9] Herath, T. and H.R. Rao, "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness". Decision Support Systems, 47(2), 2009, pp. 154-165.

[10] G. Dhillon, "Principles of Information Systems Security: Text and Cases", John Wiley and Sons, NY, 2007.

[11] Cavusoglu, H., H. Cavusoglu, and S. Raghunathan, "Economics of IT Security Management: Four Improvements to Current Security Practices", Communications of the Association for Information Systems", 14, 2004, pp. 65-75.

[12] Eisenhardt, K. M. and S.L. Brown, "Competing on the Edge: Strategy as Structured Chaos", Long Range Planning, 31, 1998, pp. 786-789.

[13] Dhillon, G. and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives", Information Systems Journal, 11(2), 2001, pp. 127-153.

[14] Johnston, A.C. and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study", MIS Quarterly, 34(3), 2010, pp. 549-566.

[15] Guo, K.H., N.P. Archer, and C.E. Connelly, "Understanding nonmalicious security violations in the workplace: a composite behavior model", Journal of Management Information Systems, 28(2), 2011, pp. 203-236.

[16] Hagen, J.M., E. Albrechtsen and J. Hovden, "Implementation and effectiveness of organizational information security measures", Information Management & Computer Security, 16(4), 2008, pp. 377-397.

[17] Siponen, M., S. Pahnila, and A. Mahmood, "Compliance with Information Security Policies: An Empirical Investigation", Structural Equation Modeling, 5(2), 2010, pp. 5-8.

[18] Staw, B.M. and J. Ross, "Understanding Behavior in Escalation Situations", American Association for the Advancement of Science, 246(4927), 1989, pp. 216-220.

[19] Keil, M., B.C.Y. Tan, K-K. Wei, V. Tuunainen, and A. Wassenaar, "A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects", MIS Quarterly, 24 (2), 2000, pp. 299-325.

[20] Mähring, M., M. Keil, "Information Technology Project Escalation: A Process Model", Decision Sciences, 39(2), 2008, pp. 239 – 272.

[21] Olivera, F., P.S., Goodman, and Sh. Swee-Lin Tan, "Contribution Behaviors in Distributed Environments", MIS Quarterly, 32(1), 2008, pp. 23-42.

[22] Park, S. Ch., M. Keil, J.U. Kim, and G-W. Bock, "Understanding overbidding behavior in C2C auctions: an escalation theory perspective", European Journal of Information Systems, 2012, pp. 1-21.

[23] Gefen, D., D. Straub, and M. Boudreau, "Structural Equation Modeling and Regression: Guidelines for Research Practice", Communications of the AIS, 4, 2000, pp. 1-77.

[24] Ringle, C., M. Sarstedt, and D. Straub, "A Critical Look at the USE of PLS-SEM in MIS Quarterly", MIS Quarterly, 36, 2012, pp. iii-xiv.

[25] Straub, D., M. Boudreau, and D. Gefen, "Validation guidelines for IS positivist research", Communications of the AIS, 13, 2004, pp. 380-427.

[26] Moore, G. and I. Benbasat, "Development of an Instrument to Measure the Perceptions of Adopting and

Information Technology Innovation", Information systems research, 2, 1991, pp. 192-222.

[27] W. Chin, "Commentary: Issues and Opinion on Structural Equation Modeling", MIS Quarterly, 22(1), 1998, pp. vii-xvi.

11. Appendix A

Table 3. Cross loadings

	CE	GI	Intention	SC
Insider	0.36509	0.32607	0.48606	0.35141
Outsider	0.79780	0.70935	0.99995	0.72293
CE-1	0.98991	0.82951	0.79013	0.87086
CE-2	0.98997	0.80946	0.78415	0.85841
CE-3	0.98895	0.81221	0.79353	0.87120
GI-1	0.86523	0.90559	0.77151	0.81596
GI-2	0.49043	0.73248	0.45082	0.54456
GI-3	0.66276	0.86334	0.51075	0.67105
SC-1	0.83388	0.72496	0.71557	0.92331
SC-2	0.83780	0.73425	0.70737	0.9382
SC-3	0.78327	0.76876	0.6315	0.91798
SC-4	0.80283	0.76885	0.63678	0.91724
SC-5	0.60078	0.65298	0.48954	0.71817

Table 4. Cronbach's α, composite reliability, AVE, and latent variable correlations

	α	CR	AVE	CE	GI	SC
CE	0.989	0.993	0.979	**0.990**		
GI	0.785	0.874	0.701	0.826	**0.837**	
SC	0.930	0.948	0.787	0.876	0.823	**0.887**

α = Cronbach's Alpha; **CR** = Composite Reliability; **AVE** = Average Variance Extracted; **CE** = Completion Effect; **GI** = Goal Incongruency; **SC** = Sunk Cost

Table 5. Measurement items and loadings

Constructs	Items	Mean	STD	Loading
Completion Effect	**CE**			
	CE-1	1.78	1.61	0.989914
	CE-2	1.77	1.65	0.989972
	CE-3	1.74	1.65	0.988955
Goal Incongruency	**GI**			
	GI-1	1.71	1.74	0.905596
	GI-2	2.00	1.72	0.732483
	GI-3	1.40	1.17	0.863345
Sunk Cost	**SC**			
	SC-1	1.85	1.17	0.923313
	SC-2	1.89	2.10	0.9382
	SC-3	1.54	1.59	0.917986
	SC-4	1.51	1.85	0.917242
	SC-5	2.23	1.04	0.718172
Intentions to Contact the Experts	**Intention**			
	Insiders	N/A	N/A	0.486063
	Outsiders	N/A	N/A	0.99995

Table 6. Survey Instrument

Construct	**Measurement Items**
Completion Effect	I believe that I would be successful if I continue working on my task, even if I have to break the rules of the information security policy.
	I had come too far to stop working on my task, even if I have to break the rules of the information security policy.
	I cannot abandon my task because it is near completion, even if I have to break the rules of the information security policy.
Goal Incongruency	I would choose to complete this project which is likely to be beneficial for me even if some information security policy is violated.
	I prefer not to put myself in a disadvantaged situation by not completing the task even if some information security policy is violated.
	Completion of this project is likely to serve my interests despite it might not serve the interests of my organization.
Sunk Cost	It would be regrettable for me to stop working on my task due to the effort I

	have already spent, even if I have to break the rules of the information security policy.	
	It would be regrettable for me to stop working on my task because of the time I have already spent, even if I have to break the rules of the information security policy.	
	I cannot stop working on my task due to the effort I have already spent, even if I have to break the rules of the information security policy.	
	I cannot stop working on my task due to the time I have already spent, even if I have to break the rules of the information security policy.	
	Overall, it would have been a waste of time and effort if I stopped working on my task, even if I have to break the rules of the information security policy.	
Insiders' Intentions	Would you contact the expert within the organization:	Via email
		On the phone
		Face-to-face
Outsiders' Intentions	Would you contact the expert outside the organization:	Via email
		On the phone
		Face-to-face