7-15-2012

Towards A Cross-Cultural Model Of Online Whistle-Blowing Systems Use

Paul Benjamin LOWRY
Department of Information Systems, College of Business, City University of Hong Kong, China, paul.lowry.phd@gmail.com

Kamel ROUIBAH
Department of Quantitative Methods & Information Systems, College of Business Administration, Kuwait University, Kuwait City, Kuwait, ghallawy@gmail.com

Greg MOODY
Department of Management Information Systems, Lee Business School, University of Las Vegas-Nevada, Las Vegas, Nevada, USA, greg.moody@gmail.com

Mikko SIPONEN
IS Security Research Centre, Department of Information Processing Science at the University of Oulu, Oulu, Finland, msiponen@tols16.oulu.fi

TOWARDS A CROSS-CULTURAL MODEL OF ONLINE WHISTLE-BLOWING SYSTEMS USE (RESEARCH-IN-PROCESS)

Paul Benjamin LOWRY, Department of Information Systems, College of Business, City University of Hong Kong, China, Paul.Lowry.PhD@gmail.com

Kamel ROUIBAH, Department of Quantitative Methods & Information Systems, College of Business Administration, Kuwait University, Kuwait City, Kuwait, ghallawy@gmail.com

Greg MOODY, Department of Management Information Systems, Lee Business School, University of Las Vegas-Nevada, Las Vegas, Nevada, USA, greg.moody@gmail.com

Mikko SIPONEN, IS Security Research Centre, Department of Information Processing Science at the University of Oulu, Oulu, Finland, msiponen@tols16.oulu.fi

Abstract

Whistle-blowing has long been an important organizational phenomenon that improves organizations in the long-run. Online whistle-blowing systems are becoming increasingly prevalent channels for reporting organizational abuses. Given that the Sarbanes-Oxley Act and similar financial laws throughout the world require multi-national firms to establish whistle-blowing procedures and systems, whistle-blowing research is even more important (Ernst & Young 2009). Existing whistle-blowing theory does not explicitly predict risk, trust, cross-cultural considerations, nor use of anonymous, online whistle-blowing systems. Yet, all of these are key considering in the whistle-blowing act and whistle-blowing in general. Furthermore, unless these systems are further understood, they may not be used, or they may not be used properly. This is a particular problem for multi-national financial firms that increasingly need to comply with whistle-blowing regulations.

This research-in-process paper details our plans to create and extend baseline whistle-blowing theory, by uniquely considering anonymity, risk, trust, and cross-cultural considerations in using whistle-blowing systems. The model will be rigorously testing using working professionals in the USA, Middle East, and China. We propose our design and measures for testing the model.

Keywords: Whistle blowing, whistle blowing systems, culture, Middle East, China, USA, anonymity, trust, risk, cross-cultural comparisons

1 INTRODUCTION AND MOTIVATION

A persistent global problem receiving increasing attention is organizational fraud and abuse (Bowen, Call, & Rajgopal, 2010). A key means of uncovering such fraud and abuse is through whistle-blowing (WB), which is "the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (1995, p. 680). WB is a high-risk organizational phenomenon that is misunderstood because it actually improves organizations and society in the long-run, and thus is considered increasingly important in practice and in the literature (Miceli, Near, & Dworkin, 2008; Near & Miceli, 1995).

To better understand what predicts WB of organizational abuse, researchers have developed whistle-blowing theory (WBT) (Near & Miceli, 1985). A key distinction of WBT is that it explains that an individual does not choose to whistle-blow based on a cost-benefit calculus because there are few, if any, personal benefits of WB. In fact, the risk of verbal abuse, intimidation, and being fired are very high for whistle-blowers in large organizations—despite the many global regulations protecting them (Bowen, et al., 2010). Instead, WBT focuses on whether someone determines something to be worthy of reporting and whether or not that person believes he or she has a personal responsibility to whistle-blow following an incident. Examples of applications of this theory include reporting bad news in problematic software projects and reluctance around software project problem escalation (Keil, Im, & Mähring, 2007; Keil, et al., 2010).

In recent years, legislation such as the Sarbanes-Oxley Act in the United States and similar legislation in other countries have required multinational public companies to establish channels through which whistle-blowers can anonymously report abuses (Bowen, et al., 2010; Ernst & Young, 2009). For succinctness, we term the full range of organizational fraud, abuse, misconduct, deviance, and unethical behaviour as *organizational abuse*.

Although an established stream of research has developed WBT to explain conventional WB behaviour, this theory is not designed to explain the use of anonymous WB reporting systems (WBRS) —a unique phenomenon that introduces a unique set of factors that challenge organizations. Unless these systems are further understood, they may not be used, or they may not be used properly. WBRS allow users to submit WB reports anonymously online via the Web from any place that has Internet connectivity. WBRS are differentiated from traditional means and non-computerized systems of WB—such as telephone hotlines and post office boxes—because they require interaction with a system, which introduces a unique set of user perceptions (Moore & Benbasat, 1991). Further, research on mediation communications has found that increased distance and technology mediation between the communicators makes it more difficult to communicate. Specifically, communicators have more difficulty in creating a shared context and transferring information, and are prone to experience more conflict within their relationship (Hinds & Bailey, 2003; Hinds & Mortensen, 2005). The increased difficulty in creating a shared context and transferring information increases the likelihood of miscommunication (Rogers & Lea, 2005), thus undermining the effectiveness of such systems. Given the even sharing of information, increased likelihood of conflict, and a lack of a shared context, WBRS have additional hurdles to overcome than the traditional means for WB.

By using WBRS, additional issues related to trust and risk need to be considered that provide for several compelling organizational research opportunities. First, though anonymity is assumed to be a critical part of WBRS requirements (Ernst & Young, 2009), extant WBT does not directly address anonymity. Second, though people are believed to be more likely to whistle-blow if they feel they can trust the authority to which they report (Smith & Keil, 2003), trust in the receiving authority or in the WBRS itself has not been directly model in extant WBT though it is implied throughout the literature. Third, though perceived risk of reporting is central to WB because of the high-risk nature of WB (Miceli & Near, 1984; Miceli & Near, 1985), risk is not explicitly modelled (but again is extensively implied and assumed) in extant WBT and is potentially increased through WBRS use. Fourth, the factors have not been considered together in a cross-cultural context, which is increasingly important because global WB laws apply to a large portion of multi-national companies where culture could come in conflict with WBRS use.

Given these compelling gaps in the extant WB literature, our research objectives are as follows: (1) Establish risk of reporting and risk to the employee's organization as key risk determinants of WB; (2) Establish disposition to trust, trust in the reporting tool, and trust in the report-receiving party as the key elements of trust in WB; (3) Establish how the five dimensions of anonymity affect risk, trust, and willingness to whistle blow; (4) Establish how the cross-cultural dimensions of power distance, uncertainty avoidance, collectivism-individualism all affect risk, trust, and willingness to WB.

2 BACKGROUND AND THEORY

Given these compelling gaps in extant WBT, we have preliminarily extended WBT to explicitly account for anonymity, trust, and risk, and have done so in the highly salient context of use of WBRS. The initial model that we have validated with preliminary data from 200 working professionals in the USA is depicted in Figure 1.

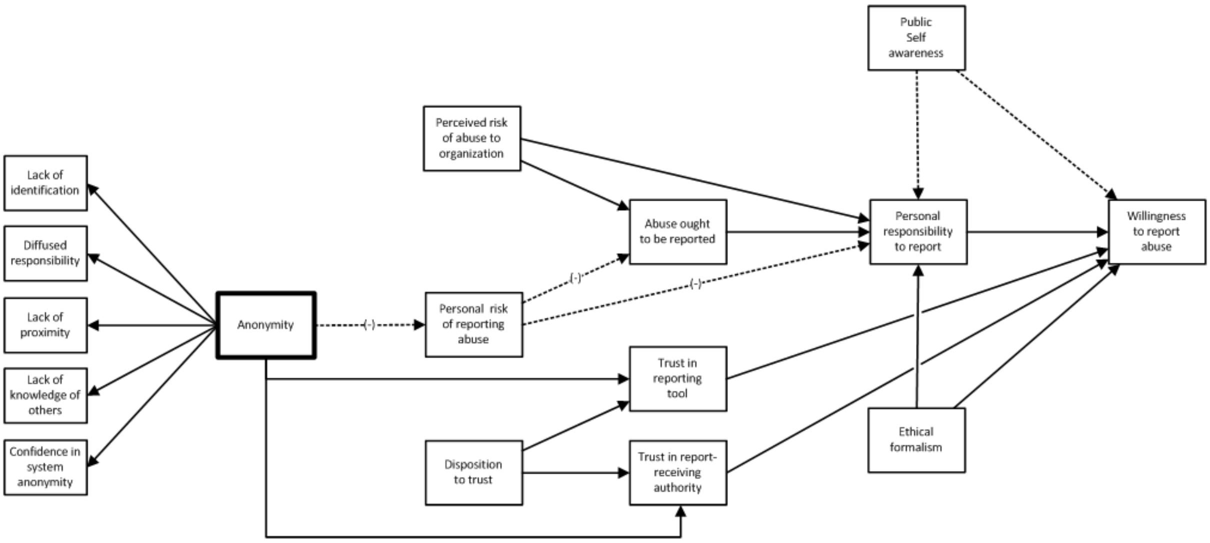

Public Self awareness
Perceived risk of abuse to organization
Lack of identification
Diffused responsibility
Lack of proximity
Lack of knowledge of others
Confidence in system anonymity
Anonymity
(-)
Personal risk of reporting abuse
(-)
Abuse ought to be reported
(-)
Personal responsibility to report
Willingness to report abuse
Trust in reporting tool
Disposition to trust
Trust in report-receiving authority
Ethical formalism

Figure 1. Preliminary Whistle-Blowing Model Validated with Preliminary USA-Based Data

The biggest limitation of the extant work in this area is that it has focused primarily on Western culture. This is particularly limiting considering that culture greatly influences attitudes and behaviours. In reviewing the literature further, we have discovered that both trust and risk—key foundations of the extended WB model—both are strongly influenced by cross-cultural considerations (e.g., Lowry, et al., 2010). Our plan is thus to create a cross-cultural WB model that can better account for the whistle blowing of participants from various cultures. The primary targets for our first round of research are the highly collectivist Middle-Eastern Arab professionals working in Kuwait and highly collectivist Chinese professionals working in China—versus highly individualist professionals working in the USA.

Prior research has theoretically and empirically demonstrated the pivotal importance of culture in information-based organizational environments (Lowry, Cao, & Everard, 2011; Lowry, et al., 2010; Posey, et al., 2010; Zhang & Lowry, 2008; Zhang, et al., 2007). The reasons for these differences are well-founded in theory and empirical studies on differences in *collectivism-individualism* (Middle Easterners and Chinese being more collectivistic; Westerners being more individualistic); *uncertainty avoidance* (Middle Easterners and Chinese desiring to avoid uncertainty more than Westerners); and *power distance* (Middle Easterners and Chinese embracing more rigid lines between people of different status, power, and rank than Westerners).

In this study, we plan on fully validating our previous (Figure 1) model with an extensive study of professionals' behaviour with WB. In addition, we are adding cross-cultural considerations on WB, as designed for comparing highly collectivist cultures versus highly individualist cultures. In doing so, we have proposed several new hypotheses to extend our model for this context. Figure 2 summarizes this new model.

The first seven hypotheses are manipulation-checks that explain based on well-established cross-cultural literature which participants will be higher and lower in which cross-cultural dimensions (e.g., Lowry, et al., 2011; Lowry, et al., 2010; Posey, et al., 2010; Srite & Karahanna, 2006; Zhang & Lowry, 2008; Zhang, et al., 2007). Based on these manipulations, we will test the path model with our cross-cultural extensions that are shaded in grey in Figure 2. Based on the extant literature, we predict participants with higher levels of collectivism, power distance, and uncertainty avoidance will perceive higher risk of reporting organizational abuse through WB. Participants that are higher in collectivism, power distance, and uncertainty avoidance will have higher trust in the report-receiving authority and trust in the reporting tool.

3 RESEARCH METHODOLOGY

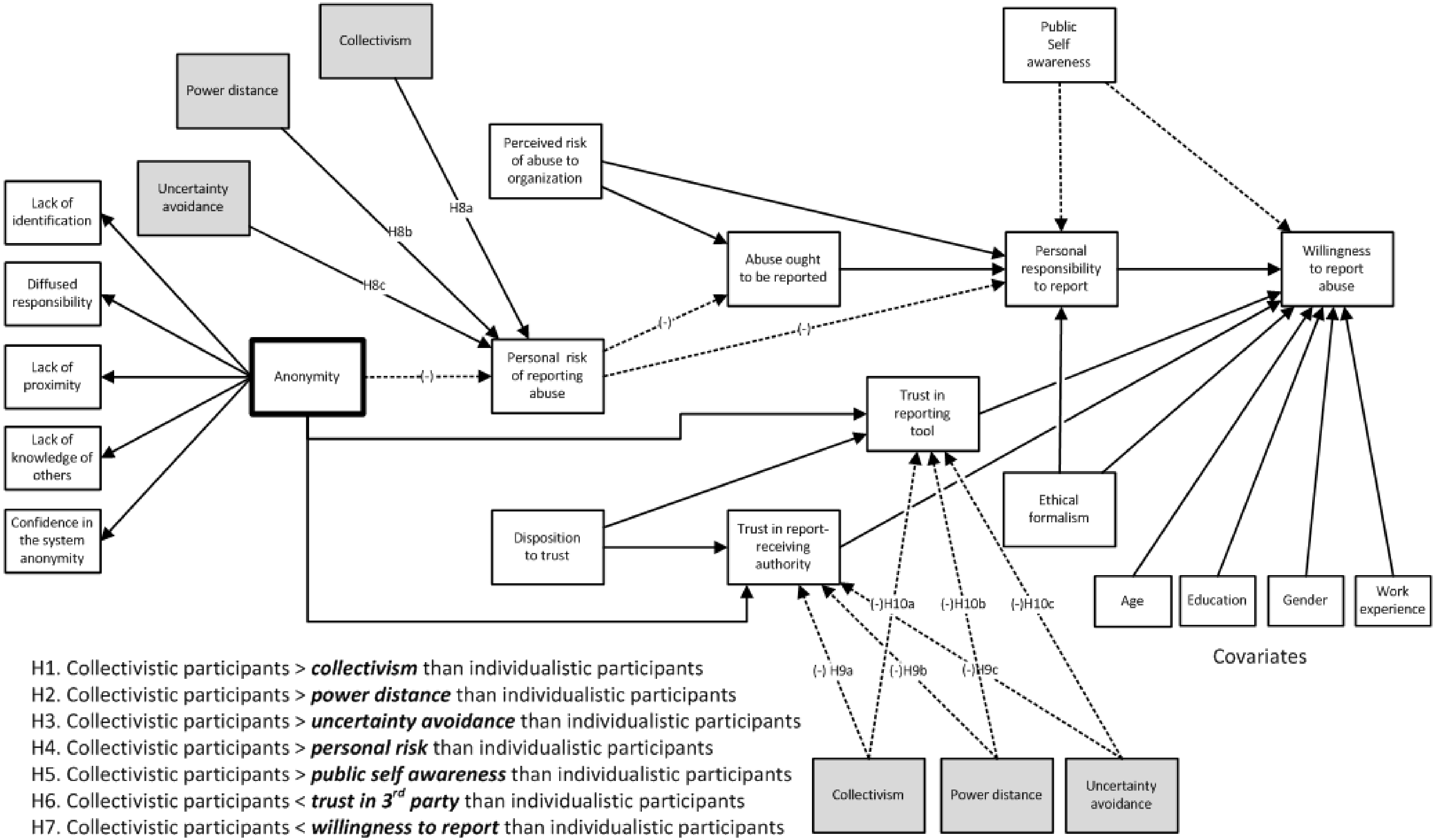
We will test our newly proposed model using two methodologies that test the same model. The first method will involve an online experiment to test participants' willingness to whistle blow, based on a hypothetical vignette. The second method will be an anonymous survey of working professionals' actual experiences with whistle blowing. The measures for both studies will be the same. The only difference will be that the first study is hypothetical whistle blowing, based on vignettes, and the second is a survey of actual whistle blowing. Because of the similarities of the two studies, for brevity we only explicate the more complicated study involving vignettes—the first study.

The first study will be an online experiment, grounded in a WB context of the highly salient organizational abuse context of computer abuse. *Computer abuse* is "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals" (Straub, 1990, p. 257). We choose computer abuse because it is a current problem that is pervasive in organizations and widely known and understood (D' Arcy, Hovav, & Galletta, 2009; Posey, et al., 2011). Computer abuse covers everything from misuse of computers at work (e.g., surfing for porn, playing games, and the like), intentionally misrepresenting system data, using organizational systems for personal profit, leaking classified information, to hacking into systems.

To test whistle blowing in a computer-abuse context, we will use a hypothetical scenario method (i.e., vignette method) to provide the treatments of our online experiment. This approach well established in studies involving questions of unethical, antisocial, deviant, and criminal behaviour. This method is likewise used frequently in management studies of computer-related abuse and ethics issues (e.g., Siponen & Vance, 2010).

3.1 Scenario Design

For increased generalizability, we have already created and pretested scenarios that were applied to actual working professionals who had to respond to a randomized, hypothetical scenario of disclosing computer abuse through a specialized reporting system in a professional setting. Our vignettes are carefully created to randomly manipulate six independent variables with two conditions each (riskiness of scenario, privacy/identification, diffused responsibility, proximity, knowledge of others, and confidence in the reporting system) to represent a range of risk and various circumstances under which the reporting would occur. Every manipulation will be randomized by the survey software to create one of 64 potential vignettes for each participant.



H1. Collectivistic participants > ***collectivism*** than individualistic participants

H2. Collectivistic participants > ***power distance*** than individualistic participants

H3. Collectivistic participants > ***uncertainty avoidance*** than individualistic participants

H4. Collectivistic participants > ***personal risk*** than individualistic participants

H5. Collectivistic participants > ***public self awareness*** than individualistic participants

H6. Collectivistic participants < ***trust in 3rd party*** than individualistic participants

H7. Collectivistic participants < ***willingness to report*** than individualistic participants

Figure 2. Proposed Cross-Cultural Collectivistic-Individualistic Model for this Study)

3.2 Scenario Testing and Pilot Test

Two rounds of data collection and expert analysis were already conducted to create appropriate scenarios that could be used to manipulate the independent variables (IVs) realistically. We first adapted and expanded on scenarios from Siponen and Vance (2010) to create a list of risky computer abuse scenarios. We then had 15 graduate students with work experience to use the risk scale from the study to rate the degree to which they believed each scenario was risky. We chose the two scenarios that were deemed to be the statistically least and most risky from this study so that perceived risk would be varied in the study (the least risky was playing a game on a computer during a company meeting; the most risky was hacking into a system). We also created wording to represent the five levels of anonymity that we will manipulate, according to the theory and instrumentation set forth by Pinsonneault and Heppel (1998). We had five experts review these manipulations to ensure that the manipulations were true to the underlying theoretical meaning of the anonymity subconstructs. We also adopted several of the experts' helpful wording suggestions. We have already pilot-tested the USA portion of the study using 148 graduate students with work experience at a large public university in the eastern United States. We also have validated the initial model in Figure 1 with 200 working professionals in the USA.

3.3 Participants

Each of two studies will involve 400 participants, for a total of 1200 participants. Each study will target 200 working Arab professionals in Kuwait, 200 working professionals in China, and 200 working professional in the USA. Each participant will only be allowed to participate in one study, and must be working full-time in jobs that involve some degree of computer use.

3.4 Measures

All of the measures for this study will be taken from established, published measures. In the pre-experiment data, we will gather background data on an individual's disposition to trust (McKnight, Choudhury, & Kacmar, 2002) the degree to which he or she has tendencies toward ethical formalism (Schminke & Wells, 1999), and the pertinent cross-cultural measures on power-distance, collectivism-individualism, and uncertainty avoidance (Srite & Karahanna, 2006). After participants receive and process their randomized scenarios, they will fill out the post-experiment scales. These included risk beliefs of the scenario and risk beliefs of reporting the incident (Jarvenpaa & Tractinsky, 1999; Malhotra, Kim, & Agarwal, 2004), public self-awareness (Pinsonneault & Heppel, 1998), the five anonymity subconstructs (Pinsonneault & Heppel, 1998), belief that the problem ought to be reported (Park, Im, & Keil, 2008), perceived responsibility to report the incident (Park, et al., 2008), willingness to report the incident (Park, et al., 2008), trusting beliefs (McKnight, et al., 2002), and trust in the computer-abuse reporting tool (Grazioli & Jarvenpaa, 2000). In addition to these measures, we will gather several covariates from the literature.

Acknowledgements

We appreciate funding support for this research stream from the City University of Hong Kong Strategic Research Grant (SRG) #2011SRG131 and City University of Hong Kong UCG Grant #7200256, as well as support from the Department of Information Systems, City University of Hong Kong.

References

Bowen, R. M., Call, A. C., & Rajgopal, S. (2010). Whistle-blowing: Target firm characteristics and economic consequences. *The Accounting Review, 85*(4), 1239-1271.

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

Ernst & Young (2009). European fraud survey 2009: Is integrity a causalty of the downturn? Retrieved from http://www.ey.com/Publication/vwLUAssets/European_fraud_survey_-_2009/$FILE/FIDS_European_fraud_survey_2009.pdf

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics--Part A: Systems and Humans, 30*(4), 395-410.

Hinds, P. J., & Bailey, D. E. (2003). Out of sight, out of sync: Understanding conflict in distributed teams. *Organization Science, 14*(6), 615-632.

Hinds, P. J., & Mortensen, M. (2005). Understanding conflict in geographically distributed teams: The moderating effects of shared identity, shared context, and spontaneous communication. *Organization Science, 16*(3), 290-307.

Jarvenpaa, S. L., & Tractinsky, N. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer Mediated Communication, 5*(2), 1-36.

Keil, M., Im, G. P., & Mähring, M. (2007). Reporting bad news on software projects: the effects of culturally constituted views of face-saving. *Information Systems Journal, 17*(1), 59-87.

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.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 165-204.

Lowry, P. B., Zhang, D., Zhou, L., & Fu, X. (2010). Effects of culture, social presence, and group composition on trust in technology-supported decision-making groups. *Information Systems Journal, 20*(3), 297-315.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

Miceli, M. P., & Near, J. P. (1984). The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis. *Academy of Management Journal, 27*(4), 687-705.

Miceli, M. P., & Near, J. P. (1985). Characteristics of organizational climate and perceived wrongdoing associated with whistle-blowing decisions. *Personnel Psychology, 38*(3), 525-544.

Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). *Whistle-blowing in organizations*. New York, NY, USA: Routledge.

Moore, G., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192-222.

Near, J. P., & Miceli, M. P. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics, 4*(1), 1-16.

Near, J. P., & Miceli, M. P. (1995). Effective whistle-blowing. *Academy of Management Review, 20*(3), 679-708.

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), 409-431.

Pinsonneault, A., & Heppel, N. (1998). Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *Journal of Management Information Systems, 14*(3), 89-108.

Posey, C., Bennett, R., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security, 7*(1), 24-47.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, S. (2010). The culture-influenced online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, *19*(2), 181-195.

Rogers, P., & Lea, M. (2005). Social presence in distributed group environments: The role of social identity. *Behaviour & Information Technology*, *24*(2), 151-158.

Schminke, M., & Wells, D. (1999). Group processes and performance and their effects on individuals' ethical frameworks. *Journal of Business Ethics, 18*(4), 367-381.

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

Smith, H. J., & Keil, M. (2003). The reluctance to report bad news on troubled software projects: A theoretical model. *Information Systems Journal*, *13*(1), 69-95.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, *30*(3), 679-704.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Zhang, D., & Lowry, P. B. (2008). Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems. *Journal of Global Information Management, 16*(1), 61-92.

Zhang, D., Lowry, P. B., Zhou, L., & Fu, X. (2007). The impact of individualism-collectivism, social presence, and group diversity on group decision making under majority influence. *Journal of Management Information Systems, 23*(4), 53-80.