Transactions on Replication Research

Methodological Replication DOI: 10.17705/1atrr.00028 ISSN 2473-3458

Employee Moral Disengagement in Response to Stressful Information Security Requirements: A Methodological Replication of a Coping-Based Model

John D'Arcy
University of Delaware, USA
jdarcy@udel.edu

Tejaswini Herath
Brock University, Canada
therath@brocku.ca

Myung-Seong Yim
Sahmyook University, South Korea
msyim@syu.ac.kr

Kichan Nam
American University of Sharjah, UAE
knam@aus.edu

H. Raghav Rao
University of Texas at San Antonio, USA
hr.rao@utsa.edu

Abstract:

The purpose of this study is to methodologically replicate the model presented by D'Arcy et al. (2014) using a new sampling frame that consists of employees in a single organization – a large academic institution in Canada (N = 150). This is in contrast to the original study, which used a large, demographically diverse sample of online panel respondents that spanned multiple organizations and industries. Our replication results confirm the results of the original study, and in doing so, support the theoretical position that security-related stress induces moral disengagement of information security policy (ISP) violations, which in turn increases ISP violation intention. The findings also indirectly support the viability of online panel respondents for studies of employees' security-related intentions. Having established the robustness of the D'Arcy et al. (2014) model across two sampling frames, we recommend future conceptual replications that employ alternate measures of security-related stress and more rigorous research designs that capture the relationships between security-related stress, moral disengagement, and ISP violations.

Keywords: information security policy (ISP), ISP compliance, security-related stress, moral disengagement theory, coping theory, methodological replication

The manuscript was received 8/12/2016 and was with the authors 8 months for 2 revisions.

1 Introduction

There is a longstanding view within both the information systems (IS) security scholarly and practitioner communities that more security is desirable in that it helps to ensure the confidentiality, integrity, and availability of organizational information assets. In contrast to this dominant viewpoint, which has strong empirical backing in the IS security literature (e.g., Angst et al. 2017; D'Arcy et al. 2009; Kankanhalli et al. 2003; Kwon and Johnson 2014; Straub 1990), there is emerging evidence that too much security can be a detriment to organizational IS security efforts, particularly in terms of employees' security-related behavior. In this vein, authors have documented how modern employees face a bevy of increasing information security requirements (i.e., policies, procedures, and technical controls; hereafter, security requirements), which they sometimes find to be constraining, inconvenient, and difficult to understand (Lee et al. 2016; Posey et al. 2014; Post and Kagan 2007; Puhakainen and Siponen 2010). When viewed in this negative light, security requirements have been shown to backfire by way of evoking employees' information security policy (ISP) violations and other negative security-related behaviors (D'Arcy et al. 2014; Lowry and Moody 2015; Posey et al. 2011).

In one of the more prominent papers to explore this topic, D'Arcy et al. (2014) proposed and tested a theoretical model that explains an underlying mechanism for the adverse effects of security requirements on employees' security-related behavior. Specifically, these authors drew on the technostress literature and conceptualized security-related stress (SRS) as comprised of the subdimensions of work overload, complexity, and uncertainty with regard to security requirements. Then, using coping theory as an overarching framework and drawing on moral disengagement theory, they posited that SRS induces moral disengagement of ISP violations as a coping response to SRS, which in turn increases ISP violation intention. In this manner of coping, employees respond to SRS through cognitive justifications and rationalizations of ISP violations, thereby disengaging their internal self-sanctions related to this behavior. The authors also drew on the deterrence literature and posited that perceived sanctions influence both moral disengagement and ISP violation intention in their model. Additional control variables were also included. Figure 1 and Table 1 present the model and list of hypotheses, respectively, from the D'Arcy et al. (2014) study.

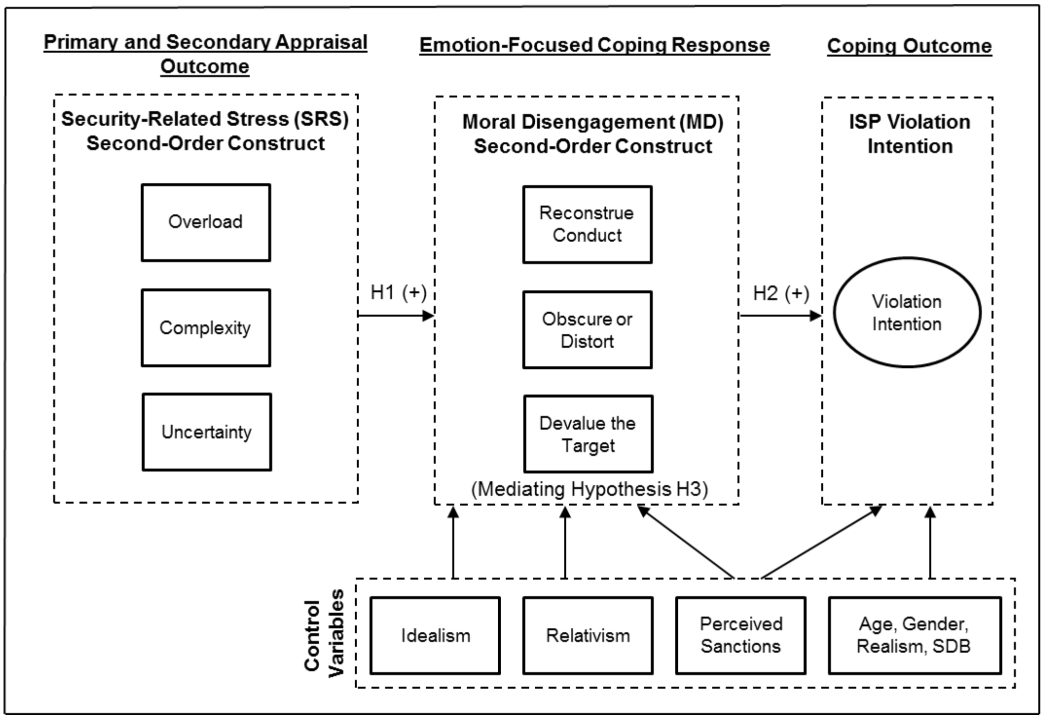

Primary and Secondary Appraisal Outcome
Emotion-Focused Coping Response
Coping Outcome
Security-Related Stress (SRS) Second-Order Construct
Overload
Complexity
Uncertainty
H1 (+)
Moral Disengagement (MD) Second-Order Construct
Reconstrue Conduct
Obscure or Distort
Devalue the Target
(Mediating Hypothesis H3)
H2 (+)
ISP Violation Intention
Violation Intention
Control Variables
Idealism
Relativism
Perceived Sanctions
Age, Gender, Realism, SDB

Figure 1. Research Model from the Original Study (D'Arcy et al. 2014)

Table 1. Hypotheses from the Original Study (D’Arcy et al. 2014)	
H1	SRS will be positively associated with moral disengagement from ISP violations.
H2	Moral disengagement from ISP violations will be positively associated with ISP violation intention.
H3	Moral disengagement from ISP violations will mediate the relationship between SRS and ISP violation intention.

To test their model, D’Arcy et al. (2014) developed an online survey instrument that contained scenarios depicting common ISP violations, along with items that measured their study constructs. An online panel provider administered the survey and the final sample consisted of responses from 539 of its panel members. The sample was comprised of computer-using professionals from the United States who worked in a wide variety of organizations that spanned multiple industries. The results supported each of D’Arcy et al.’s (2014) hypotheses, thus suggesting that SRS increases moral disengagement of ISP violations, and indirectly, increases the likelihood of ISP violations. The D’Arcy et al. (2014) study provided a significant contribution because it offered a comprehensive definition of what constitutes negative or stressful security demands, something that was lacking in the IS security literature. Moreover, the study provided a theoretical pathway to explain the adverse effects of security demands on employee behavior, and more broadly, how security requirements can backfire and negate organizational IS security efforts.

The purpose of the current study is to replicate the D’Arcy et al. (2014) model. Following the classification of replication research in Dennis and Valacich (2014), our study constitutes a methodological replication because we use exactly the same methods as D’Arcy et al. (2014) (i.e., measures, instrument, statistical analyses, etc.) but we do so with a different sampling frame. Whereas the original study used a large, demographically diverse sample (in terms of number of organizations and industries) of employees obtained through an online panel provider, we use a more traditional sampling approach for organizational studies and test the model with employees from a single organization – a large academic institution in Canada.

There are valid arguments for using both online panels and the more traditional sampling approach of obtaining employees from a single organization. Online panels provide a diversity of respondents and reduce the potential bias arising from unique organizational factors (e.g., security culture) that may be present in the data from a single organization (Bulgurcu et al. 2010). The result is increased generalizability. Obtaining respondents from a single organization, however, controls for a variety of macro-level factors that could potentially influence micro-level relationships (Karahanna et al. 1999). Following this line of reasoning, the theorized individual-level relationships (which are based on perceptual measures) that comprise the D’Arcy et al. (2014) model would be less contaminated by extraneous factors. Using employees from one or a small number of organizations has also traditionally been considered the “gold standard” of sampling approaches for survey-based organizational studies. The rationale is that the researcher has better control over and knowledge of who is actually completing the surveys (i.e., employees from a specified organization), which increases the validity of the data (Landers and Behrend 2015; Steelman et al. 2014). Notably, some scholars have contested this point and argued that one sampling approach is not necessarily better than the other; instead, the suitability of either approach is dependent on the specific research questions and boundary conditions of the study (Landers and Behrend 2015; Lowry et al. 2016). At any rate, our methodological replication of the D’Arcy et al. (2014) model with a more traditional sample provides for a triangulation of the findings of the original study. As we demonstrate in this paper, we were able to replicate the findings of the original study in the more finite context of single organization, in a different country (albeit with similar cultural characteristics; Hofstede et al. 2010), and with a smaller sample size, thus affirming the robustness of the D’Arcy et al. (2014) model across multiple contexts and supporting its external validity. We next describe the specifics of our replication study.

2 Methodology

Following the protocol of a methodological replication, we used the same scenarios and measurement items as D’Arcy et al. (2014) and replicated the design of their online survey instrument. The survey first presented respondents with one of five randomly selected scenarios describing an ISP violation. Following the scenario were items that measured scenario realism, moral disengagement (MD), perceived sanctions (PS), and ISP violation intention (INT) as each related to the ISP violation depicted in the scenario. Later in the survey were items that measured SRS, social desirability bias (SDB), ethical orientation (i.e., idealism and realism), and demographic variables. Scenario realism, SDB, and ethical orientation, along with age and gender, were used as control variables in our analysis. The scenarios and list of survey items are in Appendix A.

Survey invitations were sent to randomly selected faculty (N = 271) and staff (N = 402) employees at a large public university in southeastern Canada. As with the participants in the original study, these survey invitees constitute computer-using professionals because they use computers for large portions of their daily work activities (average of 6.3 hours per day; see Table 2).

Table 2. Demographic Profiles of Participants

Replication Study (n=150)				Original Study (n=539)			
Gender	Male	53	35%	Gender	Male	272	51%
	Female	97	65%		Female	267	49%
Age	18-24	7	5%	Age	18-24	13	2%
	25-34	24	16%		25-34	142	26%
	35-44	42	28%		35-44	129	24%
	45-54	45	30%		45-54	144	27%
	55 and over	32	21%		55 and over	111	21%
Education	High School	18	12%	Education	High School	97	18%
	Two-Year College	22	15%		Two-Year College	102	19%
	Bachelor’s Degree	44	29%		Bachelor’s Degree	214	40%
	Master’s Degree	27	18%		Master’s Degree	86	16%
	Doctoral Degree	36	24%		Doctoral Degree	21	4%
	Other	3	2%		Other	17	3%
Position	Senior Manager	12	8%	Position	Senior Manager	45	8%
	Middle Manager	20	13%		Middle Manager	118	22%
	Technical	3	2%		Technical	78	14%
	Professional Staff	80	54%		Professional Staff	134	25%
	Administrative/Other	35	23%		Administrative/Other	164	30%
Faculty or Staff	Faculty	41	27%	Industry	Manufacturing	61	11%
	Staff (Non-faculty)	109	73%		Banking/Finance	52	10%
					Information Technology	52	10%
					Healthcare	65	12%
					Government	63	12%
					Education	66	12%
					Wholesale/Retail	60	11%
					Other	120	22%
		Mean	St. dev			Mean	St. dev
Org. Tenure (years)		10.6	9.44	Org. Tenure (years)		12.3	9.56
Computer Usage (hrs./day)		6.3	1.79	Computer Usage (hrs./day)		7.5	3.53
Computer Knowledge*		5.2	0.99	Computer Knowledge*		5.5	0.97

* = Computer knowledge was self-rated on a 1-7 scale

The university employs approximately 1,500 faculty and staff employees and the list of survey invitees was compiled using the university directory and approved by the university’s institutional review board. Survey invitees received an email that contained a brief explanation of the study, a consent agreement, and a link to the online survey. Included in the invitation was the offer of entry into a lottery to win a $100 gift card for completing the survey. One hundred eighty-two employees accepted the invitation, which consisted of clicking on the link to begin the survey. Of these, 32 employees were removed due to incomplete responses or a few cases of response set biases (i.e., answers exhibiting unlikely patterns, such as all 7 or alternating

6 and 7, or survey completed in an unreasonably short time), leaving a total of 150 usable responses (22% response rate). Tests for nonresponse bias yielded no significant differences in the means of the focal study variables for the first and last third of the data, and there were no discernable differences in the eliminated versus usable responses in terms of several demographic characteristics. For comparison purposes, Table 2 provides the demographic profiles of participants in both our replication study and the original study.

Compared to the original study, our sample contained a higher percentage of females, participants with doctoral degrees, and those who identified themselves as professional staff (as opposed to the higher percentage of middle managers in the original study). The higher percentage of doctoral degrees can be attributed to the number of faculty participants. This aspect of the sample also explains the higher percentage of professional staff; the majority of faculty participants identified themselves as professional staff, regardless of their rank (e.g., clinical professor, assistant professor, associate professor, full professor). Hence, direct comparisons of the positions of several of our participants to those of the original study are not particularly relevant. Overall, our sample contained a combination of faculty and staff with varying demographic characteristics, thus capturing a broad spectrum of computer-using professionals in this particular organization.

3 Analysis and Results

3.1 Measurement Model

We used SmartPLS (version 3.2.6) to analyze the measurement and structural models. As with the original study, both SRS and MD were conceptualized as reflective second-order constructs (composed of the first-order subconstructs shown in Figure 1) and all first-order constructs in the study were reflective. Hence, our assessment of the measurement model consisted of conventional tests of convergent validity, reliability, and discriminant validity, as updated for partial least squares (PLS) analysis (Lowry and Gaskin 2014). These results are in Appendix B.

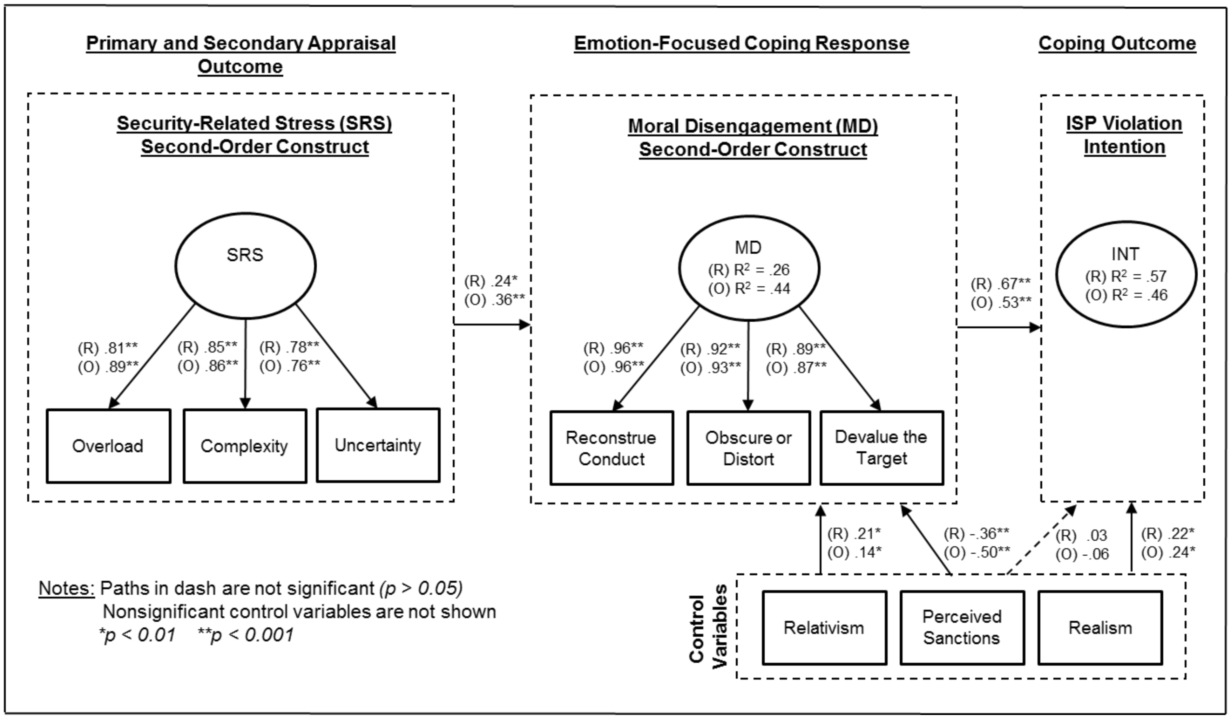
Regarding the convergent validity criterion that all items should load on their intended construct at a value of at least 0.70, we found some exceptions (see Table B1): one item each from the complexity (CX1) and uncertainty (UC1) subscales of SRS, and one item from the obscuring or distorting consequences (OC2) subscale of MD. These three items were dropped from our analysis. The same CX1 item was dropped in the original study, but the poor loadings on the UC1 and OC2 items were unique to our study. We also dropped certain items from the ethical orientation and SDB scales (see Tables A4 and B1) due to poor loadings. With two exceptions (IDEAL9 and RELA10 were not dropped in our study), these were the same items that D’Arcy et al. (2014) had to drop when using these previously validated scales. Following removal of the poor-loading items, all items met the .70 threshold for convergent validity, and the additional criterion of average variance extracted (AVE) values being at least .50 for all constructs.

For discriminant validity, the square root of AVE for each construct should be larger than the interconstruct correlations, and items should load more strongly on their corresponding construct than on other constructs. As in the original study, these conditions were met for all constructs with the exception of the first-order MD constructs. Specifically, the square root of the AVE for OC was not higher than its correlation with RC (see Table B2); and although each of the RC, OC, and DT items loaded strongest on their intended constructs, many of the loadings were not at least .10 higher than the cross-loadings (see Table B1) and there were high correlations among these constructs. These results raise concerns about discriminant validity. D’Arcy et al. (2014) found almost identical results regarding the factorial structure of these constructs, and conducted extensive supplementary analysis (available in their online appendix) to support their discriminant validity and the conceptualization of MD as a second-order construct with RC, OC, and DT as its subconstructs. Specifically, D’Arcy et al. (2014) performed a confirmatory factor analysis using EQS in which the twenty-four MD items loaded onto their respective first-order factors (RC, OC, and DT) and the three first-order factors loaded onto a single factor. The results revealed a reasonable model fit, and tests of constrained versus freely correlated pairs of first-order factors supported the discriminant validity of RC, OC, and DT. These authors also pointed to the theoretical justification for the second-order conceptualization of MD, and the fact that, even though the correlations among the first-order MD constructs were high, they were still below .90, which supports their distinctiveness (Pavlou et al. 2007). As the factorial structure of the MD items in our PLS measurement model results mirrored those of the original study, we felt comfortable moving forward with the second-order conceptualization of MD and did so in the spirit of a replication study. However, given that these discriminant validity concerns have now surfaced in two separate studies, it might be time to consider a unidimensional representation of MD in the IS security realm, as some authors have done in applying MD to other organizational contexts (Dang et al. 2017; Moore et al. 2012).

In terms of reliability, all constructs met the recommended threshold of .70 for both Cronbach's alpha and composite reliability (Table B3). We also tested for common method variance (CMV), although we inadvertently omitted the outside activity measure that was used as a marker variable in the original study. Since we did not have a suitable marker variable measure to use, we assessed CMV with the Harman one-factor test. We acknowledge the limitations of this test but conducted it in an effort to provide some assurance that CMV was not severely affecting our results. On this point, the Harman's test showed that the first factor accounted for 29.66% of the total variance in our data, which is less than 50% of the total variance, thereby suggesting that CMV was not a serious concern. We also highlight the combination of positive and negative correlations in our data (see Table B2), such as those between PS and INT and the MD subconstructs and INT, as evidence that CMV was not problematic in terms of consistency motif and acquiescence biases (Podsakoff et al. 2003).

3.2 Structural Model

Next, we tested the three hypotheses listed in Table 1 by examining the structural model. Bootstrapping with 250 resamples was performed to test the statistical significance of the path coefficients, and the second-order SRS and MD constructs were estimated using the factor scores of their first-order subconstructs as reflective indicators. Figure 2 compares the results of the path coefficients and explained variance for the replication study (R) and the original study (O).



Notes: Paths in dash are not significant *(p > 0.05)*
Nonsignificant control variables are not shown
**p < 0.01 **p < 0.001*

Figure 2. Results of the Replication Study (R) and Original Study (O)

The replication results explained approximately 57% of the variance in INT and 26% of the variance in MD. This is in comparison to the explained variances of 46% and 44%, respectively, for these same endogenous variables in the original study. As in the original study, the results of the structural model testing for the replication study supported all three hypotheses. In terms of H1, we found a positive and significant association between SRS and INT (β = .24, p < .01), although this path coefficient was a little lower and of weaker significance than in the original study (β = .24, p < .01 compared to β = .36, p < .001). For H2, we found a positive and significant association between MD and INT (β = .67, p < .001), and this path coefficient was stronger (albeit at the same significance level) than in the original study (β = .67, p < .001 compared to β = .53, p < .001). To test H3, we conducted a Sobel test using the technique described in the original study. This test statistic was significant (z = 2.38, p < .05), thereby suggesting that MD mediates the relationship between SRS and INT. This mediating effect was also confirmed in the SmartPLS output, which showed the indirect effect of SRS on INT to be significant (β = .15, p < .01).

Turning to the control variables, the results once again mirrored those of the original study. Scenario realism was significantly associated with INT (β = .22, p < .01), while age, gender, SDB, and perceived sanctions were not. Perceived sanctions had a significant negative relationship with MD (β = -.36, p < .001), which replicated this interesting finding from the original study. That is, the presence of sanctions for an ISP violation appears to decrease an employee's ability to rationalize and justify such behavior. Relativism had a significant positive association with MD (β = .21, p < .01) while the relationship between idealism and MD was not significant. The fact that these same results for ethical orientation held over two studies suggests something unique about the ISP violation context such that it negates the expected influence of idealism on the rationalization of this behavior. One speculative thought is that because employees often view security requirements as a nuisance and detriment to productivity (e.g., Posey et al. 2014), they are more likely to evoke principles of situational ethics (i.e., a relativist position) in deciding whether to morally disengage from ISP violations rather than consider the absolute ethical standards that are represented by idealism. We leave it to future research to investigate this notion. As a final note, and based on the previously described discriminant validity concerns among the MD subconstructs, we ran an additional structural model with MD specified as unidimensional and the path coefficient from MD to INT was nearly identical to those of both the replication and original studies that are shown in Figure 2. Table 3 provides a comparison of the main characteristics and results of the replication and original studies.

Table 3. Comparison of the Studies' Characteristics and Results

Characteristic	Replication Study	Original Study
Research Design	Cross-sectional survey	Cross-sectional survey
Survey Design	Online, scenario-based survey instrument	Online, scenario-based survey instrument
Population of Interest	Employed, computer-using professionals	Employed, computer-using professionals
Sampling Frame	Faculty and staff employees at a university in southeastern Canada	Employees in various organizations located throughout the United States
Sampling Approach	The researchers invited 673 randomly selected employees (271 faulty and 402 staff) to take the survey.	The online panel provider invited its panel members to take the survey. The researchers provided the inclusion criteria.
Analysis Software	SmartPLS	EQS, SmartPLS
Hypotheses Support	All three hypotheses supported	All three hypotheses supported
R^2 for Moral Disengagement	26%	44%
R^2 for ISP Violation Intention	57%	46%

4 Discussion and Conclusion

The results of this methodological replication study support the three hypotheses that comprise the D'Arcy et al. (2014) model. Hence, there is further empirical evidence for the theoretical position that SRS induces moral disengagement of ISP violations, which in turn increases ISP violation intention. In extending the findings of the original study to the context of a single organization, in a different country, and with a smaller sample size, this replication study helps affirm the external validity of the D'Arcy et al. (2014) model in that its relationships "hold at other times, in other settings, or with other individuals" (Sackett and Larson 1990, p. 430). We acknowledge that the extension to another country is not a particularly noteworthy aspect of our replication, given that Canada and the United States are culturally similar (Hofstede et al. 2010), but we highlight the smaller sample size as evidence that the findings of the original study were not simply an artifact of strong statistical power, given its large sample size (N = 539).

The most salient contribution of our study is the extension of the D’Arcy et al. (2014) model to the context of a single organization. While the model relationships held in this new context, there were some small differences in terms of the amount of variance explained in the moral disengagement and ISP violation intention constructs. In comparing the explained variance (R^2 values) for these two constructs across both studies, the replication results suggest that, beyond the influence of the constructs included in the D’Arcy et al. (2014) model, factors specific to a particular organization contribute to ISP violation intention whereas factors that are not specific to a particular organization contribute to moral disengagement of ISP violations.

The fact that we replicated the results of the original study with a more limited and mainstream sample indirectly supports the use of online panels as valid and reliable sources of data for studies of employees’ security-related intentions. As noted, obtaining participants directly from one or a small number organizations has traditionally been considered the ideal sampling strategy for organizational research, and some scholars have argued against alternative approaches, such as the use of online panel services from market research firms (e.g., Qualtrics) (Landers and Behrend 2015; Lowry et al. 2016). Our validation of the online panel responses from the original study is noteworthy and of practical importance given the increasing difficulties of obtaining corporate participation in academic research studies (Steelman et al. 2014), especially for studies of IS security (Crossler et al. 2013). Researchers should be more confident in the quality of responses obtained from online panel services, assuming appropriate filtering protocols are followed, based on the results of our study. Further, by conducting our replication with a more limited sample of employees from a single organization, we have completed the sequence described by Steelman et al. (2014) in which model testing and scale development are first conducted using a large and diverse sample before attempting additional validation using a more mainstream or limited sampling frame. In this vein, in addition to confirming the D’Arcy et al. (2014) model relationships, we found that the psychometric properties, construct validity, and reliability of the measurement scales held across the new sample from a single organization.

Having established the robustness of the D’Arcy et al. (2014) model across two sampling frames, we recommend that future research focus on conceptually replicating its theoretical relationships. One recommendation is to utilize alternate measures of SRS, such as physiological measures, as have been used in recent studies of work stress (Bono et al. 2013) and IS-enabled stress (Galluch et al. 2015). This is in contrast to the current measurement of SRS, which captures the concept more indirectly based on the perceived stressful demands imposed upon the employee. Researchers could then assess whether these alternate (and more direct) measures of SRS are related to moral disengagement, and indirectly to ISP violations. Conceptual replications should also utilize objective and/or independent measures of ISP violations, as opposed to the self-reported, perceptual measures that were used in both the original and replication studies.

A key limitation of this study, as with the original, is its cross-sectional design. This design represents a ‘snapshot’ approach to understanding the relationships between SRS, moral disengagement, and ISP violation intention. As organizational research has characterized stressful workplace encounters as events that vary from one point in time to another (Rodell and Judge 2009), it is likely that a more dynamic and longitudinal research design is needed to better capture the complexity of the SRS appraisal process and its coping responses. This relates to the earlier point regarding the need for conceptual replications of the D’Arcy et al. (2014) model that employ alternate measures and more advanced research designs.

In closing, the D’Arcy et al. (2014) model can be generalized to a broad range of computer-using professionals that span multiple organizations and industries. Our replication study extends the external validity of the model and provides some assurance of the viability of online panels for studies of employees’ security-related intentions. Given that security requirements are increasing and becoming a more pervasive aspect of employees’ daily work lives, we contend that research in this domain should continue and be expanded. We recommend conceptual replications of the D’Arcy et al. (2014) model as a future step toward this endeavor.

Acknowledgments

This replication study was supported in part by the Social Sciences and Humanities Research Council (SSHRC) of Canada (Grant no: 410-2010-18489).

References

Angst, C., Block, E., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter: Accounting for the influences of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, 41(3), 893-916.

Bono, J.E., Glomb, T.M., Shen, W., Kim, E., & Koch, A.J. (2013). Building positive resources: Effects of positive events and positive reflection on work stress and health. *Academy of Management Journal*, 56(6), 1601-1627.

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), 523-548.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32(1), 90-101.

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

D'Arcy, J., Herath, T., & Shoss, M.K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 291-325.

Dang, C.T., Umphress, E.E., & Mitchell, M.S. (2017). Leader social accounts of subordinates' unethical behavior: Examining observer reactions to leader social accounts with moral disengagement language. *Journal of Applied Psychology*, 102(10), 1448-1461.

Dennis, A.R., & Valacich, J.S. (2014). A replication manifesto. *AIS Transactions on Replication Research*, 1(1), 1-15.

Galluch, P.S., Grover, V., & Thatcher, J.B. (2015). Interrupting the workplace: Examining stressors in an information technology context. *Journal of the Association for Information Systems*, 16(1), 1-47.

Hofstede, G., Hofstede, G.J., & Minkov, M. (2010). *Cultures and Organizations: Software of the Mind, 3rd edition*. New York: McGraw-Hill.

Kankanhalli, A. M., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139-154.

Karahanna, E., Straub, D.W., & Chervany, N.L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), 183-213.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, 38(2), 451-471.

Landers, R. N., & Behrend, T. S. (2015). An inconvenient truth: Arbitrary distinctions between organizational, Mechanical Turk, and other convenience samples. *Industrial and Organizational Psychology*, 8(2), 142-164.

Lee, C., Lee, C.C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59, 60-70.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, 57(2), 123-146.

Lowry, P.B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal*, 25(5), 433-463.

Lowry, P.B., D'Arcy, J., Hammer, B., & Moody. G. (2016). Cargo cult science in traditional organization and information systems survey research: A case for nontraditional methods of data collection, including Mechanical Turk and online panels. *Journal of Strategic Information Systems*, 25(3), 232-240.

Moore, C. Detert, J.R., Trevino, L.K., Baker, V.I., & Mayer, D.M. (2012). Why employees do bad things: Moral disengagement and unethical organizational behavior. *Personnel Psychology*, 65(1), 1-48.

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, 31(1), 105-136.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., & Podsakoff, N.P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.

Posey, C., Bennett, R.J., & Roberts, T.L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6), 486-497.

Posey, C., Roberts, T.L., Lowry, P.B., & Hightower, R.T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, 51(5), 551-567.

Post, G.V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3), 229-237.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778.

Rodell, J.B., & Judge, T.A. (2009). Can "good" stressors spark "bad" behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors. *Journal of Applied Psychology*, 94(6), 1438-1451.

Sackett, P.R., & Larson, J. (1990). Research strategies and tactics in I-O psychology. In Dunnette, M.D. & Hough, L. (Eds.), *Handbook of industrial and organizational psychology, 2nd edition* (pp. 19-89). Palo Alto, CA: Consulting Psychologists Press.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 38(2), 355-378.

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

Appendix A: Survey Instrument

Table A1. ISP Violation Scenarios

Password sharing scenario: Jim is an employee in your organization. One day while Jim is out of the office on a sick day, one of his co-workers needs a file on Jim's computer. The co-worker is of equal rank and performs similar job functions to Jim. The co-worker calls Jim and asks for the password. Although Jim knows that your organization has a policy that passwords must not be shared, he shares his password with the co-worker.

Password write down scenario: Lee is an employee in your organization. The organization recently installed a computer system for managing employee personal information (for example, employee emergency contacts, retirement benefits, salary information). Each employee has been given their own username and password for the system. Lee is aware of the company policy stating that users are required to keep their passwords to themselves and not let other people know or use them. However, finding it difficult to remember his password, Lee wrote it down on a sticky note and attached it to the computer he usually uses.

Failure to logoff scenario: Pat is an employee in your organization. As part of his job, Pat has been given authorized access to the company's payroll system. One day at work, Pat logs into the payroll system to gather information for a weekly report that he prepares for management. After some time, Pat is in need of a restroom break. He is aware of the company's policy that requires users to logoff their computers when not in use. However, Pat hates the inconvenience of logging out and logging back in again, so he does not log off his computer when he leaves his desk to visit the restroom.

USB copy scenario: Chris is an employee in your organization and is currently working on a report that requires the analysis of sensitive company data. He is extremely busy and wants to continue working on the report later that evening at home. Chris is aware of your company's policy that prohibits users from copying company data to portable media, such as USB drives, to avoid security problems. However, Chris copies several company files to his personal, unencrypted USB drive so that he can work on the report at home.

Data leakage scenario: Alex is an employee in the human resources department at your organization and thus has been authorized to view the salary information of all employees as part of his job functions. Recently, one of Alex's friends (who does not work for your organization) contacted Alex and asked for the salary information of all managers in your organization. The friend informed Alex that he was applying for a management position in your organization and wanted to use the information to determine what salary to ask for in case he is offered the position. Although Alex believes that providing the salary information is a violation of company policy, he looks it up and gives it to the friend.

Table A2. Scenario-Specific Items

Item#	Item
INT1	How likely is it that you would have done the same as Jim in that situation? (very unlikely/very likely)
INT2	I could see myself sharing the password as Jim did: (strongly disagree… strongly agree)
PS1	What is the likelihood that Jim would be formally punished? (very unlikely/very likely)
PS2	Jim would be reprimanded at some point for sharing the password: (strongly disagree/strongly agree)
PS3	If punished, how severe would Jim's punishment be? (not severe at all/very severe)
PS4	Jim would receive harsh sanctions for sharing the password: (strongly disagree/strongly agree)
PS5	If punished, Jim's punishment would be immediate: (strongly disagree/strongly agree)
PS6	If punished, Jim's punishment would be timely: (strongly disagree/strongly agree)
RC1	It is alright to share a password to get work done quicker.
RC2	It is alright to share a password if it helps you do your job more efficiently.
RC3	It is alright to share a password when you are in a hurry and the work needs to get done.
RC4	It is not such a bad thing to share a password if the situation calls for it.
RC5	Password sharing is really just a reality in the workplace.
RC6	Sharing a password with a co-worker is no big deal.
RC7	An employee's good job performance should compensate for occasional policy violations such as sharing a password.
RC8	Sharing a password is no big deal when you consider that more severe policy violations happen all of the time.
RC9	Compared to other security policy violations, password sharing is minor.

Table A2. Scenario-Specific Items - Continued

OC1	Employees cannot be blamed for sharing a password if they are overloaded with work tasks.
OC2*	If management does not want password sharing, they should put in place better workarounds.
OC3	Employees cannot be blamed for sharing passwords because it is difficult to get the job done otherwise.
OC4	An employee cannot be blamed for sharing a password because many factors contribute to this action.
OC5	It is unfair to blame one employee for sharing a password when many others do the same.
OC6	It is unfair to blame one employee for sharing a password because he/she has limited responsibility for information security.
OC7	Sharing a password really won't hurt the organization.
OC8	Giving a password to a co-worker if he/she needs it doesn't really do any harm.
OC9	It is ok to share a password because no direct damage is done to the company.
DT1	If feel it is ok to violate policy, such as sharing a password, because my company is so bureaucratic.
DT2	My organization is really not people-oriented, so I don't mind violating a policy that prohibits password sharing.
DT3	Violating policy, such as sharing passwords, is fine because my company lacks consideration for its employees.
DT4	It is ok to share a password because a policy that prohibits this action is too restrictive.
DT5	It is ok to share a password because a policy that prohibits this action is unreasonable.
DT6	It is ok to share a password because a policy that prohibits this action is too strict.

INT = ISP Violation Intention; PS = Perceived Sanctions; RC = Reconstruing the Conduct; OC = Obscuring or Distorting Consequences; DT = Devaluing the Target
Notes: (1) the above items followed the scenario, in scrambled order; (2) the items above pertain to the password sharing scenario - item wordings were slightly modified to fit each scenario; (3) all items were measured using a seven-point scale and the items for the RC, OC, and DT constructs had "strongly disagree" and "strongly agree" as anchors; (4) * = item dropped from final analysis.

Table A3. Security-Related Stress (SRS) Items

Item#	**Item**
CX1*	I sometimes feel pressure in my job due to information security requirements.
CX2	I find that new employees often know more about information security than I do.
CX3	I do not know enough about information security to comply with my organization's policies in this area.
CX4	I often find it difficult to understand my organization's information security policies.
CX5	It takes me awhile to understand my organization's information security policies and procedures.
CX6	I sometimes do not have time to comply with my organization's information security policies.
OL1	I am forced by information security policies and procedures to do more work than I can handle.
OL2	My organization's information security policies and procedures hinder my very tight time schedules.
OL3	I have a higher workload due to increased information security requirements.
OL4	I am forced to change my work habits to adapt to my organization's information security requirements.
UC1*	There are constant changes in information security policies and procedures in my organization.
UC2	There are frequent upgrades to information security procedures in my organization.
UC3	There are always new information security requirements in my job.
UC4	There are constant changes in security-related technologies in my organization.

CX = SRS-Complexity; OL = SRS-Overload; UC = SRS-Uncertainty
Notes: (1) the above items followed the scenario-specific items, in a separate section, in scrambled order; (2) all items were measured using a seven-point scale with "strongly disagree" to "strongly agree" as anchors; (3) * = item dropped from final analysis.

Table A4. Ethical Orientation and Social Desirability Bias Items

Item#	Item
IDEAL1	People should make certain that their actions never intentionally harm another even to a small degree.
IDEAL2	Risks to another should never be tolerated, irrespective of how small the risks might be.
IDEAL3	The existence of potential harm to others is always wrong, irrespective of the benefits gained.
IDEAL4	One should never psychologically or physically harm another person.
IDEAL5	One should not perform an action which might in any way threaten the dignity and welfare of another individual.
IDEAL6	If an action could harm an innocent other, then it should not be done.
IDEAL7*	Deciding whether or not to perform an action by balancing the positive consequences of the act against the negative consequences is immoral.
IDEAL8	The dignity and welfare of the people should be the most important concern in any society.
IDEAL9	It is never necessary to sacrifice the welfare of others.
IDEAL10*	Moral behaviors are actions that closely match the ideals of the most “perfect” action.
RELA1*	There are no ethical principles that are so important that they should be a part of any code of ethics.
RELA2	What is ethical in society varies from one situation to another.
RELA3*	What one person considers moral may be judged to be immoral by another.
RELA4*	Different types of morality cannot be compared as to “rightness.”
RELA5	Questions of what is ethical for everyone can never be resolved since what is moral or immoral is up to the individual.
RELA6	Moral standards are simply personal rules that indicate how a person should behave and are not to be applied in making judgments of others.
RELA7	Ethical considerations in interpersonal relationships are so complex that individuals should be allowed to formulate their own ethical codes.
RELA8	Rigidly codifying an ethical position that prevents certain types of actions could stand in the way of better human relations.
RELA9	No rule concerning lying can be formulated; whether a lie is permissible or not totally depends on the situation.
RELA10*	Whether a lie is judged to be moral or immoral depends upon the circumstances surrounding the action.
SDB1	I am always courteous even to people who are disagreeable.
SDB2	No matter who I’m talking to, I’m always a good listener.
SDB3	I am always willing to admit it when I make a mistake.
SDB4*	I have never intensely disliked anyone.
SDB5	I would never think of letting someone else be punished for my wrongdoings.

IDEAL = Idealism; RELA = Relativism; SDB = Social Desirability Bias
Notes: (1) the above items followed the items in Tables A2 and A3, in a separate section, in scrambled order; (2) all items were measured using a seven-point scale with “strongly disagree” to “strongly agree” as anchors; (3) * = item dropped from final analysis.

Appendix B: Measurement Model Analysis

Table B1. Factor Loadings and Cross-Loadings

Item	OL	CX	UC	RC	OC	DT	INT	PS	IDEAL	RELA	SDB
OL1	**-0.86**	0.54	0.30	0.07	0.08	0.13	0.05	0.13	0.03	0.01	-0.08
OL2	**-0.88**	0.52	0.35	0.09	0.11	0.17	0.09	0.20	0.03	0.06	0.01
OL3	**-0.82**	0.53	0.36	0.04	0.02	0.12	0.09	0.12	0.10	-0.04	0.03
OL4	**-0.71**	0.56	0.37	0.14	0.18	0.18	0.18	0.11	0.10	0.14	0.00
CX1*	0.72	**-0.56**	0.42	-0.02	-0.01	0.08	0.08	0.15	0.05	0.02	0.00
CX2	0.45	**-0.70**	0.40	0.10	0.17	0.20	0.18	0.01	0.16	0.05	0.03
CX3	0.39	**-0.73**	0.36	0.21	0.22	0.21	0.17	0.08	0.19	0.04	0.04
CX4	0.34	**-0.72**	0.40	0.15	0.16	0.13	0.12	0.03	0.23	-0.09	0.12
CX5	0.39	**-0.78**	0.41	0.06	0.13	0.16	0.14	-0.10	0.17	0.00	0.08
CX6	0.53	**-0.79**	0.25	0.18	0.22	0.27	0.23	0.07	-0.06	0.00	-0.03
UC1*	0.10	0.04	**-0.51**	-0.10	-0.05	-0.09	-0.07	0.05	-0.06	0.02	0.03
UC2	0.37	0.46	**-0.83**	-0.01	0.01	0.04	0.04	0.19	0.20	0.09	0.06
UC3	0.27	0.41	**-0.86**	-0.05	-0.02	0.00	0.07	0.22	0.24	-0.03	0.13
UC4	0.45	0.53	**-0.87**	-0.02	0.00	0.02	0.05	0.17	0.27	-0.03	0.13
RC1	0.09	0.17	-0.01	**-0.90**	0.82	0.75	0.71	-0.33	-0.09	0.08	-0.16
RC2	0.12	0.20	-0.04	**-0.95**	0.80	0.73	0.67	-0.33	-0.11	0.14	-0.23
RC3	0.07	0.13	-0.05	**-0.91**	0.77	0.76	0.66	-0.32	-0.12	0.08	-0.20
RC4	0.02	0.13	-0.01	**-0.93**	0.74	0.67	0.65	-0.34	-0.12	0.16	-0.21
RC5	0.08	0.12	-0.01	**-0.74**	0.66	0.61	0.50	-0.32	0.03	0.04	-0.08
RC6	0.04	0.14	-0.07	**-0.91**	0.85	0.81	0.64	-0.35	-0.14	0.07	-0.27
RC7	0.14	0.18	0.02	**-0.82**	0.77	0.66	0.55	-0.21	-0.14	0.12	-0.20
RC8	0.13	0.14	-0.09	**-0.86**	0.81	0.74	0.53	-0.34	-0.07	0.04	-0.19
RC9	0.12	0.12	-0.05	**-0.81**	0.80	0.76	0.50	-0.35	-0.11	0.12	-0.22
OC1	0.13	0.24	0.12	0.73	**-0.81**	0.69	0.55	-0.23	-0.09	0.12	-0.16
OC2*	0.22	0.32	0.18	0.42	**-0.55**	0.42	0.31	-0.16	0.13	0.14	-0.02
OC3	0.09	0.20	0.00	0.80	**-0.88**	0.71	0.56	-0.31	-0.02	0.09	-0.18
OC4	0.05	0.12	-0.07	0.85	**-0.89**	0.75	0.61	-0.32	-0.05	0.15	-0.20
OC5	0.14	0.13	0.09	0.67	**-0.70**	0.61	0.41	-0.26	-0.01	0.08	-0.09
OC6	0.15	0.26	-0.04	0.77	**-0.84**	0.82	0.53	-0.29	0.01	0.07	-0.12
OC7	0.02	0.10	-0.08	0.79	**-0.83**	0.75	0.48	-0.36	-0.15	0.11	-0.26
OC8	0.03	0.17	-0.08	0.88	**-0.89**	0.81	0.67	-0.35	-0.16	0.11	-0.23
OC9	0.08	0.15	-0.11	0.80	**-0.89**	0.73	0.61	-0.32	-0.08	0.09	-0.20
DT1	0.19	0.27	0.11	0.73	0.73	**-0.84**	0.59	-0.25	-0.12	0.06	-0.25
DT2	0.22	0.23	0.04	0.65	0.68	**-0.84**	0.52	-0.23	-0.11	0.05	-0.25
DT3	0.16	0.23	0.03	0.67	0.70	**-0.85**	0.49	-0.28	-0.09	0.09	-0.22
DT4	0.09	0.18	-0.06	0.75	0.78	**-0.87**	0.63	-0.29	-0.12	0.10	-0.18
DT5	0.19	0.24	0.00	0.86	0.86	**-0.93**	0.64	-0.28	-0.05	0.08	-0.16
DT6	0.13	0.19	-0.03	0.85	0.85	**-0.91**	0.65	-0.27	-0.05	0.08	-0.17
INT1	0.13	0.22	0.05	0.73	0.68	0.70	**-0.96**	-0.31	-0.03	-0.03	-0.03
INT2	0.11	0.21	0.06	0.63	0.60	0.62	**-0.98**	-0.26	0.00	-0.08	-0.06

Table B1. Factor Loadings and Cross-Loadings - Continued

PS1	0.18	0.09	0.21	-0.35	-0.33	-0.28	-0.26	**-0.89**	0.07	0.05	0.00
PS2	0.18	0.08	0.22	-0.31	-0.30	-0.29	-0.22	**-0.85**	0.05	0.03	0.00
PS3	0.14	0.04	0.21	-0.35	-0.32	-0.28	-0.29	**-0.88**	0.07	0.04	0.05
PS4	0.11	-0.03	0.14	-0.38	-0.36	-0.31	-0.31	**-0.89**	0.04	0.10	0.04
PS5	0.17	0.03	0.16	-0.25	-0.26	-0.20	-0.19	**-0.75**	0.04	0.01	0.15
PS6	0.10	0.02	0.18	-0.18	-0.20	-0.15	-0.17	**-0.71**	0.04	0.07	0.12
IDEAL1	0.07	0.17	0.19	-0.08	-0.06	-0.10	-0.03	0.10	**-0.77**	-0.09	0.41
IDEAL2	0.11	0.15	0.31	-0.10	-0.08	-0.12	-0.07	0.08	**-0.84**	-0.10	0.42
IDEAL3	0.05	0.13	0.18	-0.12	-0.06	-0.08	-0.01	0.09	**-0.80**	-0.01	0.44
IDEAL4	-0.01	0.13	0.24	-0.08	-0.02	-0.06	0.03	0.01	**-0.84**	-0.18	0.54
IDEAL5	0.01	0.10	0.24	-0.09	-0.06	-0.11	0.01	-0.05	**-0.86**	-0.18	0.59
IDEAL6	0.02	0.13	0.24	-0.09	-0.02	-0.08	-0.02	0.03	**-0.83**	-0.15	0.53
IDEAL7*	0.15	0.18	0.18	-0.14	-0.11	-0.15	-0.06	0.14	**-0.51**	-0.08	0.22
IDEAL8	0.05	0.15	0.20	-0.09	-0.08	-0.10	-0.03	0.05	**-0.74**	-0.10	0.49
IDEAL9	0.12	0.17	0.11	-0.03	-0.01	0.01	0.00	0.09	**-0.70**	-0.10	0.40
IDEAL10*	0.05	0.18	0.09	-0.04	0.01	0.04	0.07	-0.06	**-0.53**	-0.31	0.31
RELA1*	0.13	0.05	-0.02	-0.03	0.00	0.03	-0.11	0.14	-0.22	**-0.41**	-0.25
RELA2	0.16	0.15	0.17	0.13	0.08	0.04	-0.03	0.07	-0.16	**-0.73**	-0.11
RELA3*	-0.08	-0.11	-0.07	0.00	0.04	-0.05	0.00	-0.03	0.07	**-0.53**	0.02
RELA4*	-0.09	-0.13	-0.03	0.02	0.07	-0.04	-0.06	0.06	-0.08	**-0.61**	-0.05
RELA5	0.04	0.03	-0.03	0.08	0.09	0.08	-0.02	0.06	0.01	**-0.74**	-0.05
RELA6	0.06	0.04	-0.01	0.04	0.04	0.06	-0.08	0.13	-0.06	**-0.77**	-0.04
RELA7	0.07	0.02	-0.02	0.08	0.08	0.13	-0.07	0.10	-0.14	**-0.71**	-0.09
RELA8	-0.08	-0.04	-0.08	0.18	0.21	0.17	0.08	0.02	-0.09	**-0.76**	-0.06
RELA9	0.05	0.04	0.12	0.11	0.13	0.08	-0.03	-0.05	-0.16	**-0.78**	-0.17
RELA10*	0.02	-0.06	0.01	0.08	0.07	0.03	-0.03	-0.11	-0.28	**-0.60**	-0.21
SDB1	-0.01	0.09	0.13	-0.08	-0.10	-0.12	0.00	0.00	0.49	-0.07	**-0.80**
SDB2	-0.01	0.06	0.03	-0.16	-0.14	-0.15	-0.04	0.05	0.50	-0.08	**-0.83**
SDB3	-0.01	0.05	0.10	-0.15	-0.12	-0.18	0.01	0.02	0.52	-0.11	**-0.82**
SDB4*	0.03	0.08	0.13	-0.25	-0.24	-0.20	-0.08	0.18	0.22	-0.11	**-0.54**
SDB5	-0.04	-0.06	0.09	-0.24	-0.21	-0.24	-0.09	0.03	0.38	-0.22	**-0.71**

Notes: * = item dropped from final analysis.

Table B1. Descriptive Statistics and Correlations

Construct	Mean	SD	1	2	3	4	5	6	7	8	9	10	11
OL(1)	2.72	1.18	**.81**										
CX(2)	3.22	1.13	.59*	**.72**									
UC(3)	3.42	1.20	.43*	.51*	**.86**								
RC(4)	3.19	1.64	.11	.20†	-.03	**.87**							
OC(5)	3.13	1.61	.11	.23*	-.02	.87*	**.85**						
DT(6)	2.49	1.40	.19†	.27*	.03	.84*	.86*	**.87**					
INT(7)	2.53	1.94	.13	.23*	.06	.64*	.66*	.67*	**.98**				
PS(8)	2.99	1.49	.18†	.02	.23*	-.36*	-.36*	-.30*	-.29*	**.83**			
IDEAL(9)	5.67	1.13	.07	.18†	.28*	-.10	-.08	-.10	-.02	.06	**.80**		
RELA(10)	3.78	1.21	.08	.06	.03	.15	.14	.13	-.04	.08	-.12	**.71**	
SDB(11)	5.93	0.87	-.02	.05	.11	-.20†	-.19†	-.22*	-.04	.04	.61*	-.14	**.79**

Notes: Bold values are square root of average variance extracted (AVE); * p < 0.01, † p < 0.05, two-tailed tests.

Table B3. Average Variance Extracted and Reliability Statistics

Second Order Construct	First Order Construct	AVE	Cronbach's Alpha	Composite Reliability
Security-Related Stress (SRS)	OL	.66	.82	.88
	CX	.52	.77	.84
	UC	.74	.82	.89
Moral Disengagement (MD)	RC	.76	.95	.96
	OC	.72	.91	.95
	DT	.76	.93	.94
	INT	.96	.96	.97
	PS	.69	.91	.93
	IDEAL	.65	.92	.93
	RELA	.50	.79	.85
	SDB	.62	.79	.86

About the Authors

John D'Arcy is an Associate Professor in the Department of Accounting & MIS in the Alfred Lerner College of Business and Economics at the University of Delaware. He holds a Ph.D. in Business Administration from Temple University, with a specialization in Management Information Systems. His research interests include information assurance and security, IT risk management, and computer ethics. His research appears in journals such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, and *European Journal of Information Systems*, among others. He serves as an associate editor at *MIS Quarterly*.

Tejaswini (Teju) Herath is an Associate Professor of Information Systems in the Goodman School of Business at Brock University, Canada. She received her Ph.D. from the State University of New York (SUNY), Buffalo. She holds a NSA certified Certificate in Information Assurance from SUNY Buffalo and has master's degrees in both Information Systems and Computer Engineering from Auburn University. Her main research interests are information security and privacy. Her research appears in journals such as *Journal of Management Information Systems*, *Decision Support Systems*, *European Journal of Information Systems*, *Information Systems Journal*, and *Journal of Business Ethics*, among others.

Myung-Seong Yim is an Assistant Professor in the Department of Business Administration at Sahmyook University in Seoul, South Korea. He holds a Ph.D. in Management Information Systems from Sogang University. His research interests include the dark side of IT, service innovation, service systems, and research methods in the IS field. His research has been presented at international conferences, such as the *Hawaii International Conference on Systems Sciences*, and appears in journals such as *European Journal of Information Systems* and *IEEE Transactions on Professional Communication*.

Kichan Nam is a Professor in the Department of Marketing and Information Systems at American University of Sharjah, UAE. He received his Ph.D. in Management Information Systems from the State University of New York (SUNY), Buffalo. His major research topics are IT outsourcing, e-business, IT service management, e-government, and smart tourism. His publications are found in major international journals such as *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, and *Decision Support Systems*, among others. He was Chairman of itSMF Korea, Chairman of the Korean IT Outsourcing Forum, and Vice President of the Korean Society of MIS.

H. Raghav Rao is the AT&T Distinguished Chair in Infrastructure Assurance and Security at The University of Texas at San Antonio (UTSA) College of Business. He also holds a courtesy appointment as full professor in the UTSA Department of Computer Science. He received his Ph.D. from Purdue University. His research interests are in the areas of decision support systems, e-business, emergency response management systems, and information assurance. He has authored or co-authored more than 200 technical papers, of which more than 125 are published in archival journals. He is chair of the IFIP WG 8.11/11.13 working group for Information Systems Security Research and co-editor in chief of *Information Systems Frontiers*, associate editor at *ACM Transactions on Management Information Systems*, and senior editor at *MIS Quarterly*.