Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00027 ISSN 2473-3458

Protection Motivation and Deterrence: Evidence from a Fortune 100 Company

David Sikolia
Illinois State University
David.Sikolia@ilstu.edu

Douglas Twitchell
Boise State University
DougTwitchell@boisestate.edu

Glen Sagers
Illinois State University
gsagers@ilstu.edu

Abstract:

This paper contains a conceptual replication of Herath and Rao (2009), who tested the Integrated Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) model of security policy compliance under the umbrella of the Decomposed Theory of Planned Behavior (DTPB). This study replicates their research model except for the Response Cost construct. In contrast to the original study, all data for this replication comes from a single organization, and the survey instrument references a security policy specific to this organization, not generic security policies in multiple organizations. Our results, based on 437 observations, confirm some of the original findings but not all. Relationships stemming from Organizational Commitment, Resource Availability, Security Breach concern level and Subjective Norms are similar across both studies. The findings for other relationships drawn from PMT, GDT, and TPB are mixed. We believe that the evidence provided in this conceptual replication of the Integrated Model (Herath & Rao, 2009) supports the robustness of parts of the model. We encourage future research and practice to focus on replicating and confirming the parts of the model that are similar in both studies.

Keywords: Security policy compliance, protection motivation, deterrence, organizational commitment

The manuscript was received 06/01/2016 and was with the authors 11 months for 3 revisions.

1 Introduction

Numerous industry studies and surveys indicate that information systems (IS) security is a top managerial concern (Willison & Warkentin, 2013). One of the key problems affecting the security of information systems in organizations is the insider, the trusted employee or contractor with valid access to systems. The academic community has responded to these concerns by undertaking research focusing on organizational information security practices as well as individual security behaviors.

This paper is a replication of one such study, (Herath & Rao, 2009). Their paper draws from the areas of Protection Motivation Theory, General Deterrence Theory, and Organizational Behavior to develop and test an Integrated Protection Motivation and Deterrence model of security policy compliance under the umbrella of the Theory of Planned Behavior. Their integrated model examines security compliance in a more holistic manner, which in our opinion is worthy of replication.

The replication we perform is not an exact replication. It is a conceptual replication, whereby we test the same hypotheses, but in a different context, and with a different analysis of the data. (Dennis & Valacich, 2014). As noted in Dennis and Valacich's (2014) manifesto, this type of replication can be the strongest form of replication, since it applies the same concepts across multiple groups with different cultures. In this replication, we test their entire model except one construct. Thus, there are three main differences between the studies. First, while Herath and Rao (2009) administered the instrument to employees at a variety of organizations, our replication focused on a single company. Second, because of this focus, we slightly altered the questions to refer to a specific corporate security policy, rather than to security policies generally. Third, the policy we referred to had recently been changed, a change that affected all employees on the company network with Internet access. These changes allow us to see whether the model is robust when used in a single specific environment, when referring to a specific policy, and when that policy has recently changed. Boundary conditions specific to each of the studies are summarized in Table 1. These are aspects of the "who, where, and when" of the model (Busse, Kach, & Wagner, 2016).

Table 1. Boundary Conditions

	Herath and Rao (2009)	**This Study**
Number of organizations contacted	690	1
Number of organizations indicating interest	120	1
Number of organizations that actually participated	78	1
Number of employees in each organization	10	1070
Number of usable responses	312	437

According to Deterrence Theory (Straub, 1990), individuals weigh the costs and benefits before engaging in criminal behavior and choose crime if it pays. Thus, if an individual concludes that there is a high probability of being caught and the punishment is severe, then they will not engage in criminal behavior (Mahmood, Siponen, Straub, Rao, & Raghu, 2010; Straub, 1990). Classical deterrence theory posits that the certainty, severity, and celerity of punishment are factors that guide an individual's decision to commit or not commit a crime (Pahnila, Siponen, & Mahmood, 2007). Celerity of punishment refers to how fast punishment is delivered. General deterrence theory posits that the greater the certainty and severity of sanctions for a criminal act, the more individuals are deterred from the act (D'Arcy, Hovav, & Galletta, 2009). General deterrence theory includes three additional factors: social disapproval, self-disapproval, and impulsivity (Pahnilaa et al., 2007).

Protection Motivation Theory is rooted in fear appeals and postulates that people protect themselves based on four factors. These four factors arise from the cognitive appraisal of two processes: threat appraisal and coping response appraisal (Herath & Rao, 2009). Threat appraisal stems from the perceived severity of a threatening event, and the perceived probability of occurrence or vulnerability. Coping response appraisal stems from efficacy of the recommended preventive behavior and perceived self-efficacy (Rogers, 1975).

Rational Choice Theory proposes that offenders weigh the costs and benefits of engaging in deviant behaviors before deciding to act (Li, Zhang, & Sarathy, 2010). Individuals are sensitive to the consequences

of their behavior and make rational decisions based on a cost-benefit analysis of the intended behavior. The decision to act in an offending manner is a function of the perceived costs and perceived benefits of the criminal behavior (Hu, Xu, Dinev, & Ling, 2011). The perceived risks include detection probability, sanction severity, subjective norms, and security risks (Bulgurcu, Cavusoglu, & Benbasat, 2010).

Based on General Deterrence Theory, Protection Motivation Theory, Theory of Planned Behavior, Decomposed Theory of Planned Behavior, and Organizational Commitment, Herath and Rao (2009) developed the following 15 hypotheses.

Hypothesis 1: Attitudes towards information security policies will positively influence security policy compliance intentions.

Hypothesis 2: The perceived severity of a potential security breach will positively affect the level of security breach concern.

Hypothesis 3: The perceived probability of a security breach will positively affect the level of security breach concern.

Hypothesis 4: Higher levels of security breach concern will result in more positive attitudes towards security policies.

Hypothesis 5: The perceived effectiveness of one's actions will positively affect one's attitude towards security policies.

Hypothesis 6: The perceived response cost will negatively influence one's attitude towards security policies.

Hypothesis 7: Self-efficacy will positively influence one's attitude towards security policies.

Hypothesis 8: Self-efficacy will positively affect intention to comply with organizational information security policies.

Hypothesis 9: Resource availability will positively affect self-efficacy.

Hypothesis 10: The severity of the penalty will positively affect the intention to comply with organizational information security policies.

Hypothesis 11: The certainty of detection will positively affect the intention to comply with organizational information security policies.

Hypothesis 12: Subjective norms [expectations of relevant others] will positively affect intention to comply with organizational information security policies.

Hypothesis 13: Descriptive norms [behavior of similar others] will positively influence intentions to comply with security policies.

Hypothesis 14: Higher levels of organizational commitment will lead to higher employee perceptions of the effectiveness of their actions.

Hypothesis 15: The level of organizational commitment will positively affect the intention to follow security policies.

Figure 1 shows their research model and the results from their data analysis.

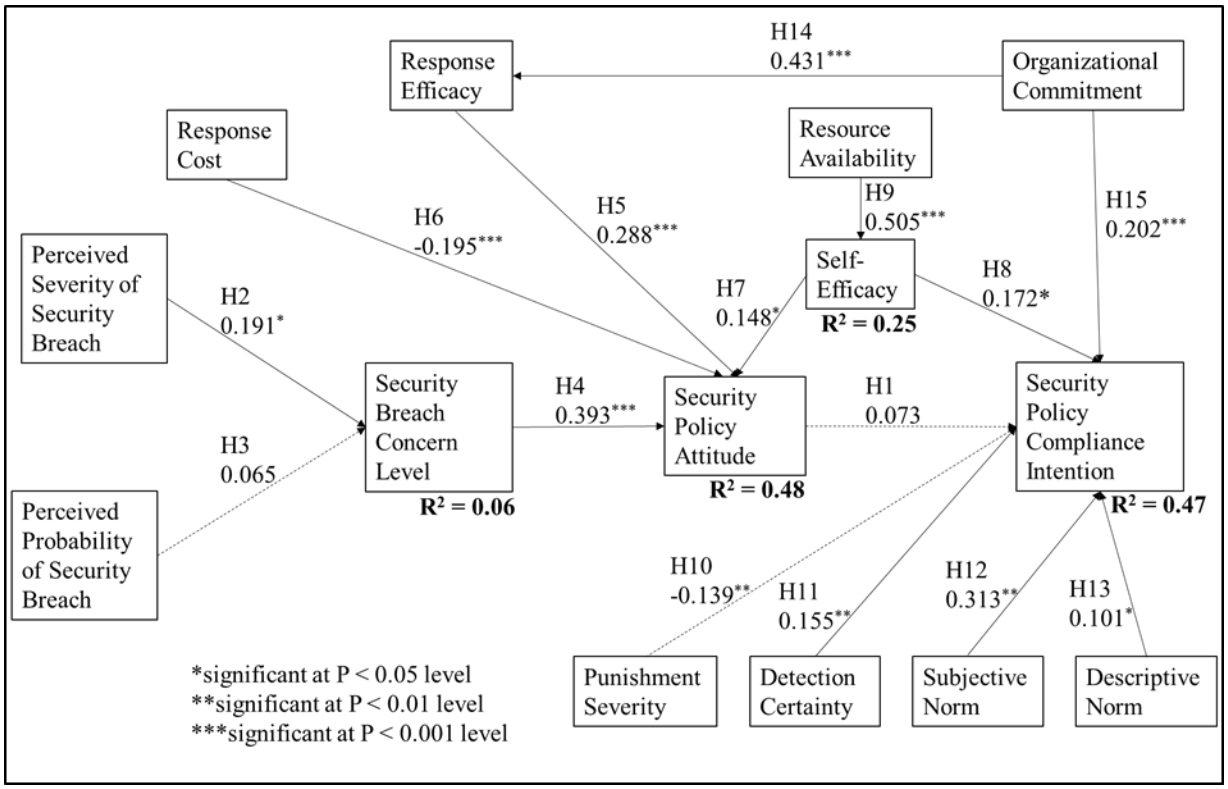

Figure 1. Original Research Model and Related Results

2 Methodology

We performed an empirical test of the relationships suggested in their research model on data we collected using a field study survey. In the following sections, we present the instrument and describe the survey administration and participants.

2.1 Instrument

We used the same instrument as the original study with adaptations to fit the specific context. The survey items were updated from referencing generic security policies in multiple companies, to wording that referred to a recent, specific policy enforcement change in a specific company. These changes to wording, and administering the survey in a single company, constitute the situational differences between the original Herath & Rao (2009) paper and this conceptual replication. The firm in which the survey was administered was a Fortune 100 company, in manufacturing and engineering. The employees to whom the survey was administered worked in all business areas of the company, not just technical areas. However, all were geographically at the same campus, not worldwide.

Several weeks before the survey was administered, the company had changed a policy enforcement mechanism concerning Internet usage throughout the company network. Prior to the change, only a Web access policy governed employees' use of the Internet from the company's network. Like acceptable use policies at many companies, it prohibited use of the company network for activities such as accessing pornographic material or promoting outside businesses. When employees attempted to access a site that was on a blacklist, the system blocked their access and logged the attempt. Excessive attempts by employees were investigated. In response to some violations that were difficult to track to individuals, the company added additional enforcement to the policy: employees were now required to login to a portal to be able to access Internet sites that were not on an approved list. The purpose of the authentication was to help in tracking violations and to remind employees of the Internet usage policy. The company reported to us that their detected violations of the Web access policy fell by 44%, but did not cease, in response to the policy requiring authentication. Our study, administered several weeks after the policy change, was intended to gauge employee response to the authentication requirement and help the company understand why the remaining violations occurred.

According to company contacts who had been directly involved in its implementation, the addition of the authentication enforcement mechanism to the Web access policy, which was done suddenly and without much warning, caused significant controversy, both because it added an annoying and cumbersome authentication step and because it emphasized the company's monitoring of Internet usage. To capitalize on this raised awareness, we included the following in our survey recruitment email:

> "In light of the changes to authenticated web access, the Firewall & Proxy server team at [company] and researchers at [university] have teamed up on a research project to better understand this and other IT security policies and their impact on the workplace. . . ."

We did not perform an explicit manipulation check but it is reasonable to assume that the controversy, the daily login requirement, the recency of the change, and the recruitment email all focused the respondents' attention on the policy and its enforcement.

We administered the survey using the company's internal web-based survey system. Unfortunately, because it was inadvertently left out of the survey, we were unable to include response cost in our model. Table 2 lists the constructs we used, their measures, and the wording of each of those measures. In place of the original wording of security violation, we used Internet usage policy violation. In place of organization, we used company. In place of security technologies, we used Internet authentication.

Table 2. Measurement Instrument

Organizational commitment	OCM1	I am willing to put in a great deal of effort beyond that normally expected in order to help this **company** to be successful.
	OCM2	I really care about the fate of this **company**.
	OCM3	For me, this is the best of all possible **companies** in which to work.
Perceived probability of security breach	IncCert1	How likely is it that an **Internet usage policy** violation will cause a significant outage that will result in the loss of productivity?
	IncCert2	How likely is it that an **Internet usage policy** violation will cause a significant outage to the Internet that results in financial losses to organizations?

	IncCert3	How likely is it that the **company** will lose sensitive data due to an **Internet usage policy** violation?
Perceived severity of security breach	IncSev1	I believe that information stored on **company** computers is vulnerable to security incidents due to **Internet usage policy** violations.
	IncSev2	I believe the productivity of the **company** and its employees is threatened by security incidents due to **Internet usage policy** violations.
	IncSev3	I believe the profitability of the **company** is threatened by security incidents due to **Internet usage policy** violations.
Security breach concern level	SecConc1	**Internet usage** issues affect my organization directly.
	SecConc2	**Internet usage** issues are exaggerated.
	SecConc3	I think **Internet usage** is a serious issue and needs attention.
Response efficacy	ResEff1	Every employee can make a difference when it comes to helping to secure the **company** information systems.
	ResEff2	There is not much that any one individual can do to help secure the **company** information systems.
	ResEff3	If I follow the organization's **Internet usage policies**, I can make a difference in helping to secure my **company** information systems.
Resource availability	ResAvail1	Assistance from the Help Desk is available when needed.
	ResAvail2	Information security policies**, like the Internet usage policy**, are made available to employees online.
	ResAvail3	Information security policies, **like the Internet usage policy** are written in a manner that is clear and understandable.
	ResAvail4	Users receive adequate security training before getting a network account.
	ResAvail5	A variety of business communications (notices, posters, newsletters, etc.) are used to promote security awareness.
Self-efficacy	SEff1	I would feel comfortable following most of the **Internet usage policy** on my own.
	SEff2	If I wanted to, I could easily follow the **Internet usage policy** on my own.
	SEff3	I would be able to follow most of the **Internet usage policy** even if there was no one around to help me.
Security policy attitude	SecPolAtt1	Adopting **Internet authentication** is important.
	SecPolAtt2	Adopting **Internet authentication** is beneficial.
	SecPolAtt3	Adopting **Internet authentication** is helpful.
Punishment severity	PunSev1	The organization disciplines employees who break **Internet usage** rules.
	PunSev2	My organization terminates employees who repeatedly break **Internet usage policy** rules.
	PunSev3	If I were caught violating the company's **Internet usage policy** I would be severely punished.
Detection certainty	DetCer1	Employee **Internet usage** is properly monitored for policy violations.
	DetCer2	If I violated the **company's Internet usage policy**, I would probably be caught.
Subjective norms	SubNorm1	Top management thinks I should follow company **Internet authentication policies**.
	SubNorm2	My immediate supervisor thinks that I should follow company **Internet authentication policies**.
	SubNorm3	My colleagues think that I should follow company **Internet authentication policies**.
	SubNorm4	The information security department thinks that I should follow **company Internet authentication policies**.
	SubNorm5	Other computer technical specialists in the organization think that I should follow **company Internet authentication policies**.
Descriptive norms	DesNorm1	I believe other employees comply with the **company's Internet authentication policies**.
	DesNorm2	I am convinced other employees comply with the **company's Internet authentication policies**.
	DesNorm3	It is likely that the majority of other employees comply with the company's **Internet authentication policies** to help protect the organization's information systems.
Security policy compliance intention	CompInt1	I am likely to follow the company's **Internet authentication policies**.
	CompInt2	It is likely that I will comply with the company's **Internet authentication** policies to protect the organization's information systems.
	CompInt3	I am certain that I will follow the company's **Internet authentication policies**.

2.2 Survey administration and participants

We received 1070 responses. Of these, 589 identified as male, 238 identified as female, the rest did not specify their gender. The table below provides the descriptive statistics. This data includes only those who reported on the specific items, so all sum to 100%.

Table 3. Descriptive Statistics

		Count	%
Gender	Female	238	28.8
	Male	589	71.2
Education	Graduate Degree	162	20.4
	Bachelor's Degree	467	58.8
	Some College	126	15.9
	High School (other)	39	4.9
Age	18 - 25	26	3.1
	26 - 35	204	24.6
	36 - 45	238	28.7
	46 - 55	232	28.0
	56 and older	128	15.5

3 Data Analysis

We used SPSS version 22 and Amos version 23 for measurement validation and to test the structural model. Amos, which employs a structural equation modelling (SEM) statistical technique, was used largely for confirmation.

We began by screening the data. The first step was to identify and remove any records with missing values. The next step was to screen for unengaged responses. Any record with a standard deviation of 0.5 or below was dropped from the data set. This process left us with a sample of size of 437. To assess common-method bias, we ran a factor analysis in SPSS with the number of factors fixed to 1 and no rotation. The un-rotated principal-component factor that emerged explained 21.12% of the variance, which is less than the critical 50%. Second, the un-rotated principal-component factor analysis revealed twelve factors with eigenvalues greater than 1. The first factor accounted for 21.12% of the variance. All twelve factors together accounted for 67.14% of the variance, indicating an acceptable level of common method variance. We assessed discriminant validity by looking at the correlation matrix. None of the correlations between the factors exceed 0.7, which is within acceptable range. The Average Variance Extracted (AVE) did not meet the 0.5 cutoff point for some of the variables; however, we decided to include all the variables in the structural model.

Table 4. Measurement Model Statistics		
Construct	**Item**	**Factor Loadings**
Organizational commitment CR = 0.810 AVE = 0.59	OCM1	.821
	OCM2	.832
	OCM3	.635
Perceived probability of security breach CR = 0.722 AVE = 0.478	IncCert1	.795
	IncCert2	.774
	IncCert3	.449
Perceived severity of security breach CR = 0.833 AVE = 0.716	IncSev1	.802
	IncSev2	.868
	IncSev3	.867
Security breach concern level CR = 0.543 AVE = 0.29	SecConc1	.400
	SecConcR	.561
	SecConc3	.630
Response efficacy CR = 0.533 AVE = 0.356	ResEff1	.721
	ResEff2	.734
	ResEff3	.091
Resource availability CR = 0.734 AVE = 0.245	ResAvail1	.195
	ResAvail2	.819
	ResAvail3	.717
	ResAvail4	.157
	ResAvail5	.325
Self-efficacy CR = 0.881 AVE = 0.712	SEff1	.839
	SEff2	.853
	SEff3	.839
Security policy attitude CR = 0.902 AVE = 0.755	SecPolAtt1	.875
	SecPolAtt2	.872
	SecPolAtt3	.860
Punishment severity CR = 0.870 AVE = 0.690	PunSev1	.849
	PunSev2	.843
	PunSev3	.799
Detection certainty CR = 0.542 AVE = 0.372	DetCer1	.601
	DetCer2	.618
Subjective norms CR = 0.845 AVE = 0.525	SubNorm1	.793
	SubNorm2	.795
	SubNorm3	.589
	SubNorm4	.768
	SubNorm5	.652
Descriptive norms CR = 0.820 AVE = 0.606	DesNorm1	.854
	DesNorm2	.829
	DesNorm3	.634
Security policy compliance intention CR = 0.818 AVE = 0.601	CompInt1	.810
	CompInt2	.690
	CompInt3	.819
CR = Composite Reliability; AVE = Average Variance Extracted		

We tested the structural model using Amos version 23. (Herath & Rao, 2009) used SmartPLS to test their structural model; we chose covariance-based structural equation modelling (CB-SEM) with Amos because our objective was to confirm that our data fit the model and because we have a larger sample. Two of the constructs, Subjective Norm and Resource Availability, are formative. Information systems literature has provided guidelines on how to analyze formative constructs via covariance-based SEM such as AMOS. The analysis requires the performance of a chi-square test on a number of models to determine which to use (Petter, Straub, & Rai, 2007). We selected the best model for the analysis (Herath & Rao, 2009), and our research hypotheses and related results are compared in Figure 2a and Figure 2b below. Like the original research, we controlled for age, education, gender, and job type.

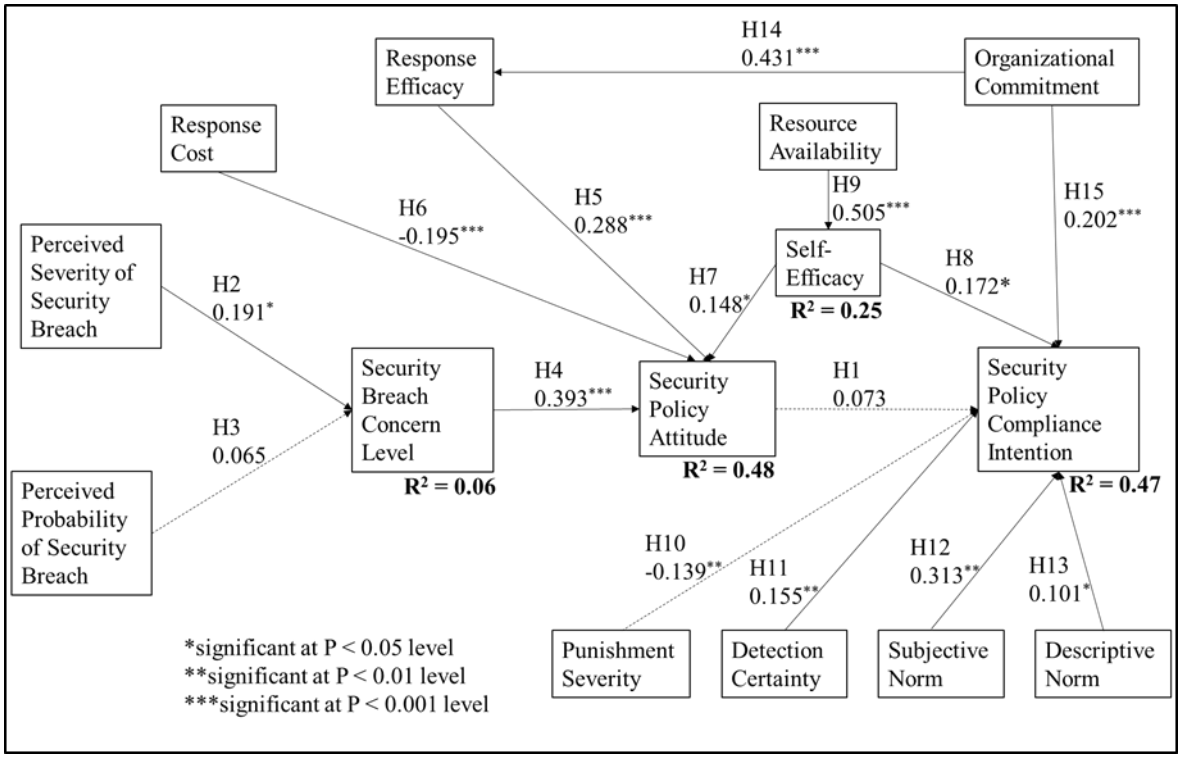

Figure 2a. Herath and Rao's (2009) Research Model and Results.

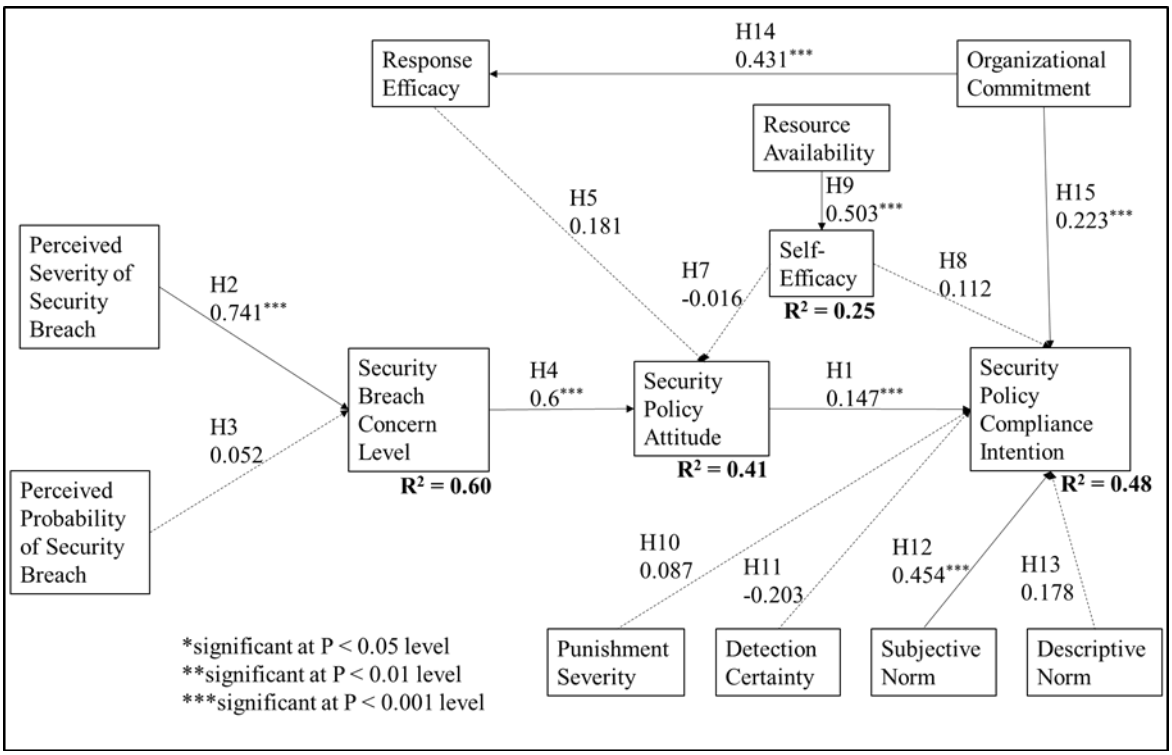

Figure 2b. Our Model and Related Results

Model fit indices meet the recommended guidelines (Gefen, Straub, & Boudreau, 2000), except for one, χ2/df. Two other indices, NFI and GFI are borderline close to the cutoff point. Table 5 suggests that the structural model has an adequate fit with the data.

Table 5. Model Fit Indices		
Fit Indices	**Heuristic**	**Model value**
χ^2		1582.590
df		773
χ^2 / df	>3.0	2.047
NFI	>0.90	0.859
GFI	>0.90	0.850
AGFI	>0.80	0.824
CFI	>0.90	0.922
RMSEA	<0.06	0.049

Our results show that nearly 48% of the variance in the security policy compliance intentions and 41% of the variance in the security policy attitude are explained in the integrated model.

4 Discussion

Table 6 compares the results of the two studies.

Table 6. Comparison of Findings			
Hypothesis	**Original Study**	**Our Study**	**Comments**
H1	0.073	0.147***	Significant in our study
H2	0.191*	0.741***	Exceptional weight in our study
H3	0.065	0.052	Similar findings
H4	0.393***	0.601***	Similar findings
H5	0.288***	0.181	Not significant in our study
H6	-0.195***		Not tested in our study
H7	0.148*	-0.016	Not significant in our study
H8	0.172*	0.112	Not significant in our study
H9	0.505***	0.503***	Similar findings
H10	-0.139**	0.087	Not significant in our study
H11	0.155**	-0.203	Not significant in our study
H12	0.313**	0.454***	Similar findings
H13	0.101*	0.178	Not significant in our study
H14	0.431***	0.431***	Similar findings
H15	0.202***	0.223***	Similar findings
*significant at P < 0.05 level, **significant at P < 0.01 level, ***significant at P < 0.001 level			

Behavioral and social sciences research involves three interrelated domains. These are the substantive domain or content; the conceptual domain which consists of the ideas that give meaning to the content; and the methodological domain which includes the techniques or procedures by which the content and ideas are studied (McGrath, 1995). Our replication study uses the same procedure as (Herath & Rao, 2009), a field study using a survey method; we tested the same concepts or research model in a different context, making this a conceptual replication. The only difference was in the content of interest; they examined a generic security policy across multiple generic organizations, whereas we examined a specific security policy in a specific organization. This may explain the differences in some of our results. In the rest of the section below, we discuss, hypothesis by hypothesis, possible theoretical reasons for the differences.

H1, H7, and H8 were drawn from three theories: the Theory of Planned Behavior (TPB), the Decomposed Theory of Planned Behavior (DTPB), and Protection Motivation Theory (PMT). Self-efficacy is the conviction that one can successfully execute the behavior required to produce the outcomes; attitude refers to the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question; and intention is an indication of an individual's readiness to perform a given behavior. Herath & Rao (2009) asked their respondents if they could easily and comfortably follow most of the IS security policies, whereas we asked our participants if they could easily and comfortably follow a specific Internet usage policy. The findings for these hypotheses are mixed, with the original study showing self-efficacy influencing both security policy attitudes and intention to comply with policies, but our study does not show the same effect. The original study found the impact of attitude on policy

compliance to be insignificant, but out study found the effect to be significant. These results may be explained by the fact that our instrument referred to specific 'Internet Usage Policy' in the Fortune 100 Company, whereas the original study referred to general IS Security policies. Individuals are prone to be more willing to comply with a specific, concrete policy, which changed in recent memory, than to comply with generic security policies with details that are at likely only vaguely remembered.

H2, H3, H4, and H5 were drawn from PMT. H6, which we did not test in our model due to inadvertent omission, was also drawn from PMT. PMT proposes that people protect themselves based on Threat Appraisal (Perceived Severity and Perceived Susceptibility) and Coping Appraisal (Perceived Response Efficacy and Perceived Self-Efficacy). The findings for H2, H3 and H4 are similar in both studies. The beta weight for H2 in our study is high, which could be explained by the high level of Internet security awareness by the participants in our study. In both studies, the certainty of security breaches has no significant impact on security concern. On the contrary, Coping Appraisal influenced attitude in their study, but not in ours. This is an interesting finding that may be explained by the recency of the Internet authentication policy in the company. A recent policy change, that seems cumbersome to use at first glance, may influence a user to be unsure about whether they will truly comply.

H12 (Subjective Norm) and H13 (Descriptive Norm) were drawn from two theories, TPB and DTPB. TPB states that attitude toward behavior, subjective norms, and perceived behavioral control work together to shape an individual's behavioral intentions. The original study found that social influence plays a role in employee security behaviors. Both studies suggest that subjective norms, or the employees' perception of what significant others think, have a significant impact on employee behaviors. However, whereas they found descriptive norms to be significant, our study provides no support for the influence of descriptive norms. In both studies, the expectations of relevant others are seen as important, but the behavior of similar others is not seen as significant in our study. In both studies the strength of the relationship is relatively small compared to that of the subjective norm. This should not be surprising given that what others do with policy compliance—especially a single policy, in a single organization (our study)—varies less than what others do among several policies and several organizations. It seems likely that what individuals think others want them to do varies strongly across individuals, and across organizations and policies.

H9 was drawn from DTPB. The findings in both studies are similar, both significant at the $p < 0.001$ level (0.505 in the original study; 0.503 in our study). Resource availability is important for employee ability to comply with security policies.

H10 and H11 were drawn from General Deterrence Theory (GDT). These results are significant in the original study but not in our study. In the original study, they found certainty of detection to have positive impact on security policy compliance intentions, and the severity of penalty was found to have a significant impact on security behavior intentions. In our study, H10 and H11 were not found to be significant. In Herath and Rao, which studied multiple organizations, fear of sanctions varied from organization to organization while our study of a single organization resulted in less variation. Since H10 and H11 were not significant in this study, we cannot state conclusively that certainty of detection and severity of punishment do not work as Herath & Rao showed, but the negative relationship we found bears further investigation.

H14 and H15 were drawn from Organizational Commitment Theory (OCT). The findings in both studies are similar, both significant at the $p < 0.001$ level (H14 was 0.431 original study and is 0.431 in our study; H15 was 0.202 in the original study and is 0.223 in our study). This seems to indicate that organizational commitment is a strong force for compliance with policy, whether in the context of a specific firm, or across multiple firms. This is unsurprising, as those with high organizational commitment tend to be good employees, who follow rules and contribute to the goals of the company.

5 Conclusion

In this paper, we present a conceptual replication of (Herath & Rao, 2009) study. As shown in Figure 2 and Table 7, several of the relationships, including those stemming from Organizational Commitment, Resource Availability, Perceived Severity, and Subjective Norms are remarkably similar across the two studies. Such consistency suggests that these relationships are robust despite the differences in the two studies. Other important relationships, however, are not consistent. The central relationships in the Theory of Planned Behavior between Concern Level and Attitude and between Attitude and Intention are, respectively,

significant but weak and not significant in Herath and Rao's (2009) results. In our results, these two are both significant and stronger than in the previous study, suggesting that the Theory of Planned Behavior may be a good fit in this context. Finally, the constructs related to General Deterrence Theory and to Punishment Severity and Detection Certainty were significant in the previous study but not in ours. This difference is likely due to the security culture and use or non-use of sanctions at the company.

We believe the evidence presented in this conceptual replication of Herath and Rao (2009) provides support for the robustness of the Integrated Protection Motivation and Deterrence model. These two studies, taken together, show that the model is robust across somewhat differing contexts and that small changes to the instrument do not invalidate the outcomes. These findings agree with a key point in Dennis and Valacich (2009): namely, they help show that there is nothing idiosyncratic about item wording. To further strengthen the theories behind the original study, future research should be conducted to validate that the constructs significant across both these studies remain significant in other scenarios. Similarly, future studies may show that both significant and non-significant constructs are not applicable in other contexts, which ultimately can lead to a more parsimonious model.

References

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.

Busse, C., Kach, A. P., & Wagner, S. M. (2016). Boundary conditions. *Organizational Research Methods,* 20(4), 574-609.

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

Dennis, A. R., & Valacich, J. S. (2014). A replication manifesto. *AIS Transactions on Replication Research, 1*(1), 1-4.

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modelling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(7), 1-79.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

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

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431-433.

McGrath, J.E. (1995) Methodology matters: Doing research in the behavioral and social sciences. *In Human–Computer Interaction: Toward the Year 2000*, R.M. Baecker, J. Grudin, W.Buxton, A., and Greenberg, S., Eds. Morgan Kaufmann Publishers, San Francisco, CA, pp.152–169.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the Proceedings of the 40th Hawaii International Conference on System Sciences, Hawaii.

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

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

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

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

About the Authors

David Sikolia is an assistant professor at Illinois State University, teaching programming and security courses. His research interests include information assurance and security. His research has appeared in peer reviewed scientific journals and conferences such as *Pacific Asia Journal of the Association of Information Systems, Journal of the Midwest Association of Information Systems*, and Americas Conference on Information Systems (AMCIS), and many others.

Douglas Twitchell is an Assistant Professor of Information Technology Management in the College of Business and Economics at Boise State University. He has published many articles in behavioral information security and other topics in outlets such as the *Journal of Management Information Systems* and *Group Decision Making and Negotiation*. As a Certified Information Systems Security Professional (CISSP) and a member of the Special Interest Group on Security in the Association for Information Systems, he enjoys keeping up with and discussing current advances in information security.

Glen Sagers is a professor in the School of Information Technology at Illinois State University. His research interests center around human factors in security and information assurance topics, such as wireless security use.