# Employees' Adherence to Information Security Policies: A Partial Replication

*Full Paper*

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

**Douglas Twitchell**
Boise State University
twitched@gmail.com

**Glen Sagers**
Illinois State University
gsagers@ilstu.edu

## Abstract

This paper conducts a partial replication of (Siponen et al. 2014) which developed a multi-theory based model that explained employees' adherence to security policies. Their paper combined elements from Protection Motivation Theory (PMT), the Theory of Reasoned Action, and Cognitive Evaluation Theory. This study is a partial conceptual replication of the PMT portion of their model. We collected our data from employees of a large mid-western university. Our results, based on 110 records contradict the findings of the original study. Where, three of the four constructs in the original study (Severity, Vulnerability, and Self-Efficacy) were found to be significant, our study found the opposite, the only significant path was Response Efficacy. Our study failed to replicate the findings in the original paper. Future studies are encouraged to methodically replicate the original study by using the same measures, treatments and statistics.

**Keywords**

Information Security policy compliance, Protection Motivation Theory, Conceptual Replication

## Introduction

Information security risks come from many fronts, both external and internal. One of the greatest concerns for Information Security managers is the insider threat(Willison and Warkentin 2013). Technical and non-technical measures have been implemented by organizations to mitigate these risks (Ifinedo 2012; Pahnilaa et al. 2007). Recent research on the topic of security policy compliance has applied a number of theories from reference disciplines. One of the theoretical lenses used is the Protection Motivation Theory (Herath and Rao 2009; LaRose et al. 2008; Lee and Larsen 2009; Pahnilaa et al. 2007; Workman et al. 2008).

Protection motivation theory of fear appeals and attitude change postulates that there are three crucial components of fear appeal. These are magnitude of noxiousness of a depicted event, the probability of the events occurrence and the efficacy of a protective response (Rogers 1975). Fear can be aroused in response to a situation that is judged threatening and thus requiring protective measures to be taken. Fear appeals has two parts; the first part contains statements articulating severity of threat and the probability of threat occurring; the second part is designed to enhance perceived efficacy by providing steps to avert the said threat and the value of averting the threat. These two cognitive processes are also referred to as the threat

appraisal and coping response appraisal. Protection motivation theory emphasizes interactions aiming to alter the way people think, feel or behave or in other words persuading them.

### *Overview of Original Research*

A number of studies on employee compliance with organizational information security policies have used Protection Motivation Theory in their research models. This study is a partial replication of (Siponen et al. 2014). Figure 1 below shows the hypotheses and results of their study.

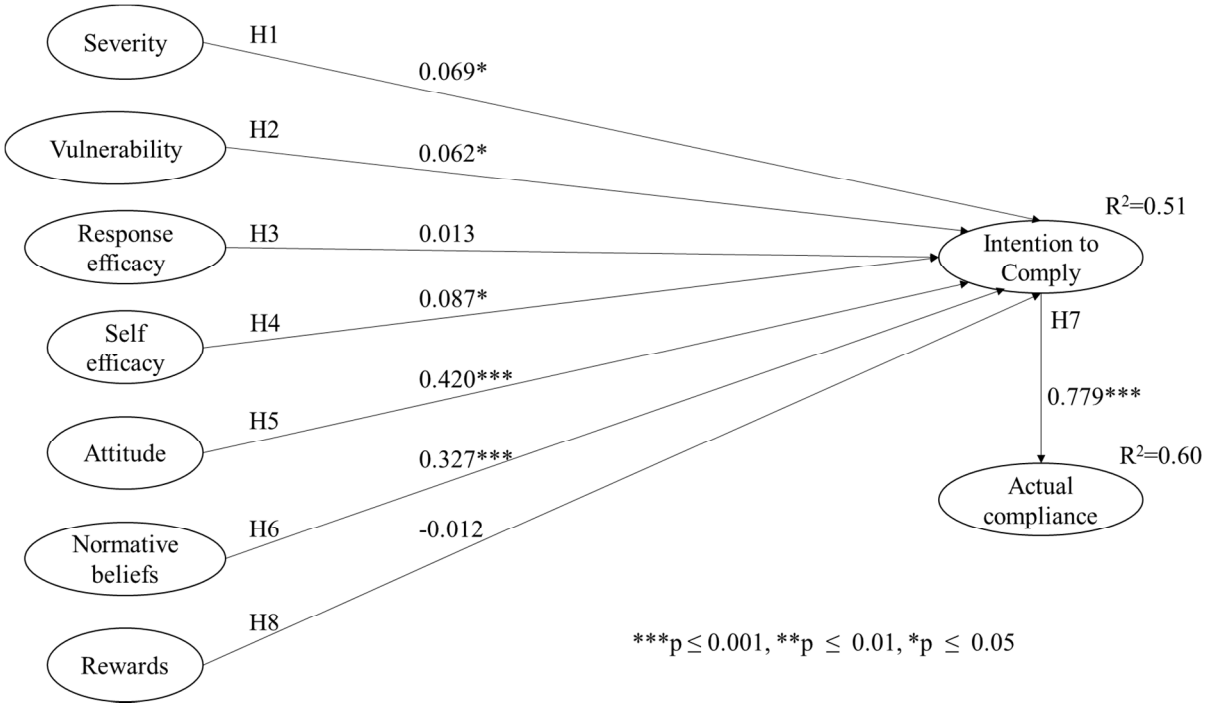


**Figure 1: Research hypothesis and related results of the replicated study**

## Research Hypothesis

Our intention is to replicate the PMT portion of the original research. We chose to only replicate the PMT portion because of the wide use of PMT in other studies and because our sample was limited in size. The PMT hypotheses, which are developed in the original research, include the following:

> *H1: Perceived severity of potential information security threats positively and significantly influence employees' intention to comply with information security policies.*
>
> *H2: Perceived vulnerability from potential security threats positively and significantly influence employees' intention to comply with information security policies.*
>
> *H3: Self-efficacy to potential information security threats positively and significantly influences employees' intention to comply with information security policies.*
>
> *H4: Response efficacy to potential information security threats positively and significantly influences employees' intention to comply with information security policies.*

## Research Methodology

Our methodology differs slightly from that of the original study making this a conceptual replication rather than a direct replication. The differences are in the sample and the questions.

The sample for this study was collected from employees at a large mid-western university. The original research's sample of 669 usable responses was obtained from employees at several companies in Finland. A total of 200 respondents were asked to complete our study. Taking into consideration missing data and invalid responses, we had 110 usable responses resulting in a high response rate of 55%.

The questionnaire items were adopted from the PMT portion of (Herath and Rao 2009), but many of the questions were modified to refer specifically to the institution's information security policies. We made this change because all of the subjects were employees of the same institution and should therefore be familiar with some of the information security policies at that institution. Furthermore, they then had a common frame of reference for the idea of an information security policy.

If PMT is a robust theory, then the effect of these changes should not be greater than the effects the theory proposes. University employees referring to specific security policies are a narrower subset of the population of employees referring to general information security policies.

| | |
|---|---|
| Severity | *IncSev1:* I believe that information stored on university computers is vulnerable to security incidents due to violation of the University information security policy.<br>*IncSev2:* I believe the productivity of the University and its employees is threatened by security incidents due to violation of the University information security policy.<br>*IncSev3:* I believe the financial standing of the University is threatened by security incidents due to violation of the University information security policy. |
| Vulnerability | *IncCert1:* Information security issues affect my organization directly.<br>*IncCert2:* Information security issues are exaggerated.<br>*IncCert3:* I think the security of information is a serious issue and needs attention. |
| Response Efficacy | *ResEff1:* Every employee can make a difference when it comes to helping to secure the the University information systems.<br>*ResEff2:* There is not much that any one individual can do to help secure the University information systems.<br>*ResEff3:* If I follow the University information security policies, I can make a difference in helping to secure my organizations information systems. |
| Self-Efficacy | *SEff1:* I would feel comfortable following most of the information security policy on my own.<br>*SEff2:* If I wanted to, I could easily follow information security policy on my own.<br>*SEff3:* I would be able to follow most of the information security policy even if there was no one around to help me. |
| Intention to Comply | *CompInt1:* I am likely to follow the University information security policies.<br>*CompInt2:* It is likely that I will comply with the University information security policies to protect the organizations information systems.<br>*CompInt3:* I am certain that I will follow the University information security policies. |

**Table 1: Measuring instrument**

## Data Analysis and Results

We used SPSS version 22 and Amos version 23 for measurement validation and to test the structural model. Amos uses a structural equation modelling (SEM) statistical technique which is largely used for confirmation. Our intention was to confirm the validity of the Protection Motivation Theory (PMT) in the context of employee compliance with organizational information security policies.

### *Common-method bias*

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 27.84% of the variance, which is less than the critical 50%. Second, the un-rotated principal-component factor analysis revealed four factors with eigenvalues greater than 1. The first factor accounted for 27.84% of the variance, the second factor 18.37%, the third factor 12.16% and the fourth 9.25%. All the four factors accounted for 67.62% of the variance. This indicates an acceptable level of common method variance.

### *Convergent and discriminant validity*

The test for the normal distribution of the data was not successful.

Convergent validity means that factors within a single factor are highly correlated. Convergent validity was examined using the pattern matrix below, which was extracted using principal-component analysis and Promax rotation. For our sample size of 110, the loadings on IncCert3 and ResEff3 are not sufficient. However, the average loading on IncCert was greater than 0.700 which is good, but less than 0.700 for ResEff which is not good.

| | Component | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| IncCert1 | .097 | .000 | .099 | **.825** | .022 |
| IncCert2 | .028 | .081 | -.013 | **.907** | .029 |
| IncCert3 | -.074 | -.195 | .404 | **.369** | .171 |
| IncSev1 | -.084 | -.154 | **.882** | -.082 | .033 |
| IncSev2 | -.005 | .073 | **.883** | .088 | -.055 |
| IncSev3 | .018 | .177 | **.770** | .092 | -.173 |
| ResEff1 | .161 | .100 | .213 | -.237 | **.673** |
| ResEff2 | .145 | -.008 | .274 | -.276 | **-.802** |
| ResEff3 | .442 | .021 | .066 | -.126 | **.380** |
| CompInt1 | **.933** | -.043 | .012 | .106 | -.012 |
| CompInt2 | **.965** | -.074 | -.005 | .077 | -.010 |
| CompInt3 | **.881** | .066 | -.130 | -.021 | -.086 |
| SEff1 | .013 | **.871** | -.017 | .016 | .010 |
| SEff2 | -.022 | **.921** | .088 | -.031 | .029 |
| SEff3 | -.036 | **.904** | -.055 | .068 | .038 |

**Table 2: Pattern Matrix**

Discriminant validity refers to the extent to which factors are distinct and uncorrelated. We examined this in two different ways. The first was the pattern matrix above, where we looked for any cross-loadings with a difference less than 0.2. Again, IncCert3 and ResEff3 were a problem. The second method was examining the correlation matrix shown below. None of the correlations between the factors exceed 0.7 which is good.

| Component | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1.000 | .317 | .218 | .077 | .370 |
| 2 | .317 | 1.000 | .083 | -.074 | .241 |
| 3 | .218 | .083 | 1.000 | .263 | .151 |
| 4 | .077 | -.074 | .263 | 1.000 | .083 |
| 5 | .370 | .241 | .151 | .083 | 1.000 |

**Table 3: Correlation Matrix**

## *Reliability*

The internal consistency was assessed using Cronbach's alpha. All the factors had a value above the 0.7 threshold except *Response efficacy* which had 0.522.

| **Construct** | **Cronbach's alpha** |
|---|---|
| Severity | .731 |
| Vulnerability | .827 |
| Response efficacy | **.522** |
| Self-efficacy | .891 |
| Intention to comply | .890 |

**Table 4: Cronbach's alpha for the constructs**

Deleting any of the *Response efficacy* items does not lead to any improvement in Cronbach's alpha that is above the 0.7 (Gefen et al. 2000) level shown in the table 5 below. However, deleting the second item raises the value to 0.613 which though poor is more acceptable. We therefore excluded ResEff2 from the structural model 1 below.

| | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Squared Multiple Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|---|
| ResEff1 | 7.79 | .882 | .451 | .229 | **.219** |
| ResEff2 | 8.35 | 1.127 | .213 | .057 | **.613** |
| ResEff3 | 7.99 | 1.000 | .358 | .195 | **.384** |

**Table 5: Item-Total Statistics**

### *Testing the structural models*

We tested two structural models. Model 1 excluded ResEff2 as explained above. [1]Model 2 excluded Incert3 and ResEff3.The goodness-of-fit of the model was tested using SPSS Amos. The fit criteria as shown in the table below suggests that the structural model has adequate fit with the data (Gefen et al. 2000).

| Fit criteria | Model 1 value | Model 2 value | Acceptable standard |
|---|---|---|---|
| CMIN/Df | 1.25 | 1.30 | <3 |
| IFI | 0.98 | 0.98 | >0.9 |
| CFI | 0.98 | 0.98 | >0.95 |
| NFI | 0.91 | 0.91 | >0.9 |
| GFI | 0.90 | 0.91 | >0.95 |
| AGFI | 0.85 | 0.85 | >0.8 |
| RMSEA | 0.047 | 0.052 | <0.05 |
| PCLOSE | 0.53 | 0.44 | >0.05 |

**Table 6: Fit indices**

The standardized regression weights for model 1 are shown in the figure 2 below. The results show that 44% of variance in policy compliance intentions was explained by our model. The findings also indicate that the paths from perceived severity of security breach, perceived probability of security breach, and self-efficacy were not significant. Of the four paths, only one was significant, response efficacy. Thus, only one of the hypothesis was supported:

> *H3: Self-efficacy to potential information security threats positively and significantly influences employees' intention to comply with information security policies.*

The standardized regression weights for model 2 are shown in figure 3 below. None of the paths in model 2 were significant.

[1] We received a number of recommendations from the reviewers. The first recommendation was the cross-loading problem in table 2. IncCert3 and ResEff3 have above 0.400 cross loading. We were asked to drop these items and rewrite the analysis. The average loading on IncCert after dropping IncCert 3 is 0.874. The average loading on ResEff after dropping ResEff3 is 0.744. Both values are above 0.700 level for testing convergent validity. For discriminant validity, we examined the pattern matrix. There was no cross loading with a difference of less than 0.2.

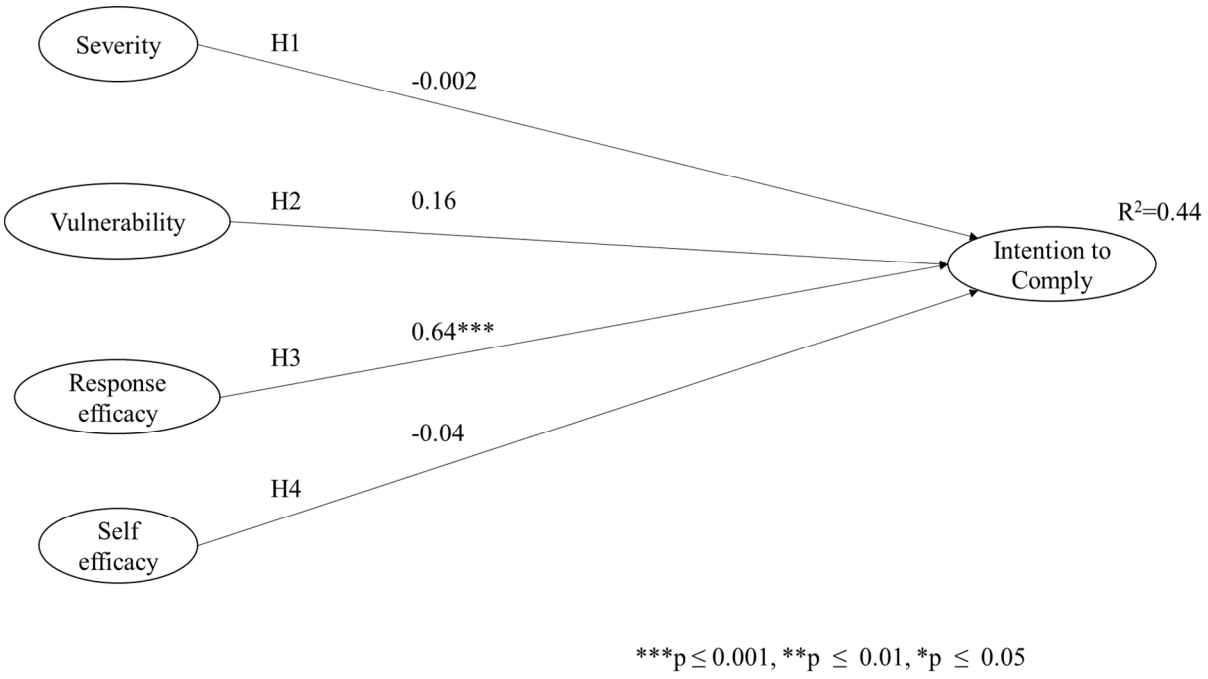


**Figure 2: Research hypothesis and related results for model 1**

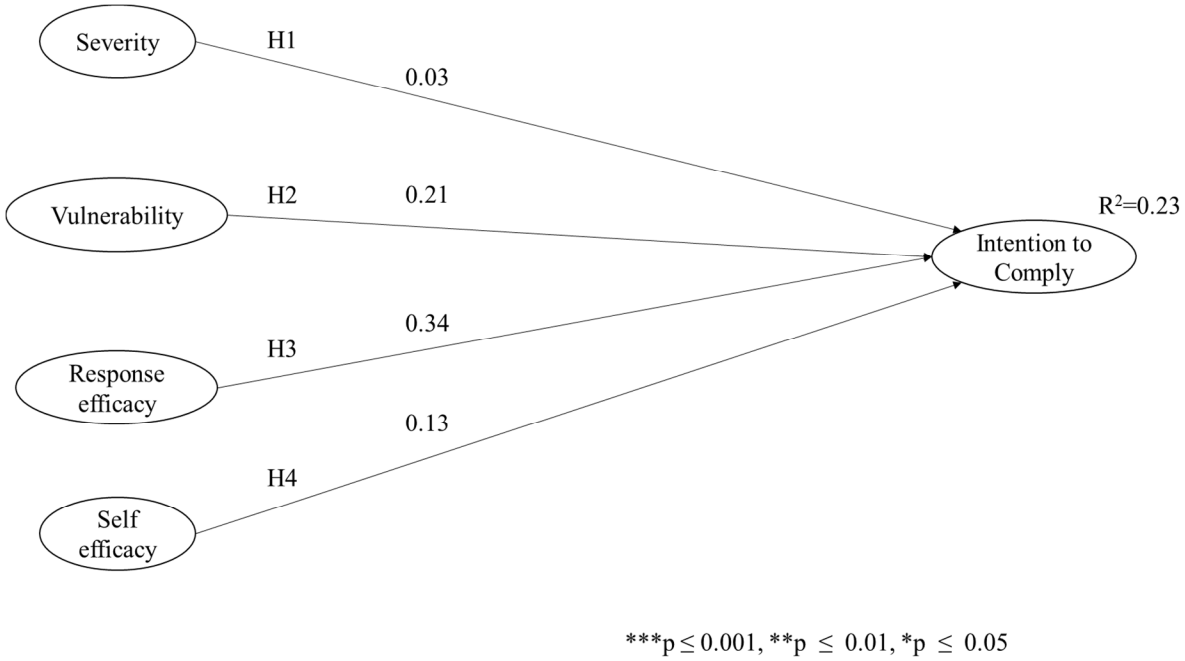


**Figure 3: Research hypothesis and related results for model 2**

## Discussion

Protection Motivation Theory (PMT) is considered a leading theory in the area of health behavior motivation. It has also been applied extensively in the area of information security policy compliance. Our study replicated one such study (Siponen et al. 2014). They developed a multi-theory based model that combined elements from Protection Motivation Theory, The Theory of Reasoned Action, and the Cognitive Evaluation Theory. They validated their model using a sample size of 669 responses from four corporations based in Finland. Their study (Siponen et al. 2014) found that perceived severity, vulnerability, and self-efficacy significantly positively impacted employees intention to comply with information security policies. Their study did not support their hypothesized positive relationship between response efficacy and intention to comply.

The results of our partial replication research contradict the findings in the original study. We tested the PMT section of their model. Our sample size of 110 responses was from employees in a single mid-western university in the US. Our data had both convergent and discriminant validity issues. We therefor analyzed two structural models, with a different set of questionnaire items dropped.

The first model of our study found the exact opposite of the original study. We found response efficacy to be significant and positively impacting intention to comply. Perceived severity, and self-efficacy did not significantly and positively impact employee's intention to comply with information security policies. Vulnerability, though positive, did not have a significant impact either. The original study showed that 51% of the variance was explained intention to comply with information security policies, whereas our model explained 44%. None of the paths in the second model were significant.

## Limitations and Implications for Future Research

This study was limited in that we did not have a large enough sample to replicate the full model in the original study. We therefore tested only part of their model that was based on protection motivation theory even though our survey included items for the other constructs. Furthermore, even though we referred to similar constructs, our questionnaire items were different. It is possible that our participants interpreted the questions differently from the participants in the original study. If this is the case, however, PMT may not be robust.

This one failed replication of PMT does not invalidate the theory. Rather, it shows that PMT may not be applicable in the specific environment we tested it in, university employees referring to specific security policies. If PMT isn't applicable in this environment, it calls into question the generalizability of PMT. If the theory is valid in some environments, but not others, it may need to be revised.

Further studies are encouraged to methodically replicate the original study. These studies should use exactly the same measures as the original study, and a larger sample size.

## REFERENCES

Gefen, D., Straub, D. W., and Boudreau, M.-C. 2000. "Structural Equation Modelling and Regression: Guidelines for Reearch and Practice," *Communications of the Association for Information Systems* (4:7), pp. 1 - 70.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Ifinedo, P. 2012. "Understanding Information Security Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and Protection Motivation Theory," *Computers & Security* (31), pp. 83 - 85.

LaRose, R., Rifon, N. J., and Enbody, R. 2008. "Promoting Personal Responibility for Internet Safety," *Communications of the ACM* (51:3), pp. 71 -76.

Lee, Y., and Larsen, K. R. 2009. "Threat or Coping Appraisal: Determinants of Smb Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems* (18), pp. 177 -187.

Pahnilaa, S., Siponena, M., and Mahmoodb, A. 2007. "Employees' Behavior Towards Is Secur Ity Policy Compliance," *Proceedings of the 40th Hawaii International Conference on System Sciences*, Hawaii: IEEE Computer Society.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), p. 93.

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51), pp. 217 -224.

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

Workman, M., Bommer, W. H., and Straub, D. 2008. "Security Lapses and Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24), pp. 2799 - 2816.