Winter 12-11-2022

Do measures of security compliance intent equal non-compliance scenario agreement?

Byron Marshall
Oregon State University, byron.marshall@bus.oregonstate.edu

Forough Nasirpouri Shadbad
Oregon State University

Michael Curry
Oregon State University

David Biros
Oklahoma State University

Do Measures of Security Compliance Intent Equal Non-Compliance Scenario Agreement?

Byron Marshall [1]
College of Business,
Oregon State University,
Corvallis, Oregon, USA

Forough Nasirpouri Shadbad
College of Business,
Oregon State University,
Corvallis, Oregon, USA

Michael Curry
School of Electrical Engineering and
Computer Science, Oregon State University
Corvallis, Oregon, USA

David Biros
Spears School of Business
Oklahoma State University
Stillwater, Oklahoma, USA

ABSTRACT

To better protect organizations from the threat of insiders, IS security (ISS) research frequently emphasizes IS Security Policy (ISP) behavior. The effectiveness of an assessment model is typically analyzed either using short survey statements (behavior survey) or by using scenario agreement (prospective scenario) to measure current and prospective compliance (or non-compliance) behavior. However, a significant gap is the lack of statistical evidence to demonstrate that these two measures or dependent variables (DV) sufficiently agree with one another. We report on an effort to compare and contrast two assessment models which employed alternate styles of DVs and demonstrate that the primary construct from two different ISS behavioral theories had approximately the same effect size on either of the DVs. Our findings add support for substantial (but not overly correlated) synchronization between the two DV values, since we also observe that the prospective scenario non-compliance measure resulted in lower model fit while the behavior survey compliance measures fit both models with higher accuracy. We discuss our findings and recommend that for many studies there can be value in employing both DVs.

[1] Corresponding author. byron.marshall@bus.oregonstate.edu +1 541-737-6054

Keywords: Information systems security (ISS) behaviors, intent to comply/violate IS Security Policy (ISP), scenario and behavior survey to measure ISP (non) compliance

INTRODUCTION

Protecting organizations from cybersecurity threats is a significant challenge. There are many threat sources to consider, but individual user behavior is widely viewed as a major contributor to information systems security (ISS) incidents and breaches (Verizon 2022). To help guide better insider's ISS behavior, organizations adopt Information Security Policies (ISPs) that communicate required and prohibited activities. Consequently, a major thrust of the IS behavioral security research is focused on contrasting end-user behavior to ISP.

ISS researchers theorize about the antecedents of behavior and then often choose one of two approaches: a focus on intention to comply/non-comply with the ISP using a set of self-reported items that measure employee general ISS intentional behavior, or reported likelihood of compliance/non-compliance with the ISP prospective of scenarios. The majority of ISS scholars utilize the former to assess employee intention to comply with ISP while the latter is used to measure employee intention to non-comply (Bulgurcu et al. 2010; Siponen and Vance 2010).

Prospective compliance (or non-compliance) and intent to (or not to) comply are both closely related and differentiated in the literature (Cram et al. 2019). Having a strong likelihood to comply generally does not preclude a preference for choosing not to comply in some circumstances (Siponen and Vance 2013). Supported by commentary in this and other previous work, it seems to us that interpretation of the research findings has assumed an overlap in the space of these two constructs when to the best of our knowledge, there is minimal statistical evidence to support such an assumption. Having a better understanding of how these two measures align could benefit cybersecurity research by providing additional guidance on when to

use behavior surveys and/or prospective scenarios. We assume that for many studies, both methods of measuring ISS behaviors (i.e., scenario-based and general self-report compliance) should be considered, and if true, then our effort to show evidence of this value would be beneficial to ISS behavior study design as well as better helping organizations effectively and efficiently assess user risk.

Hence, the research question we seek to answer is how much overlap is there between behavior surveys and prospective scenarios and can they be used interchangeably? To address our research question, we employed two validated theoretical models (technostress and role-stress) from the ISS literature (Nasirpouri Shadbad and Biros 2021; Shadbad and Biros 2020) and assessed them on two types of DVs. Following the literature, the compliance behavior was measured using a three-item construct that measures individuals' intention to comply with general ISPs. However, we used a set of scenarios to measure their ISP non-compliance behaviors in six different situations. We examined each theoretical model independently with both alternative DVs. In the later sections, we discuss the results of our analysis on how the two measures differ. We follow the discussion by providing theoretical and practical implications of this study.

BACKGROUND AND STUDY OBJECTIVE

ISS researchers have made significant contributions to understanding the antecedents of insider behavior toward ISP, and a wide range of drivers are theorized to influence these outcomes, (for reviews, see: Cram et al. 2019; Moody et al. 2018). For instance, theories such as deterrence, neutralization, and protection-motivation theories have been extensively utilized to identify contributing factors and explain how and why individuals show different behaviors in

relation to the ISPs (Mou et al. 2022; Siponen and Vance 2010; Trang and Brendel 2019). Furthermore, drawing on the person-technology fit model, recent ISS research suggested that stress resulting from ISP, technology use or job roles negatively impacts individuals' security behaviors. One notable example is work by D'Arcy et al (2014) finding that stressful environments due to ISP overload, complexity, and uncertainty result in non-compliant behaviors. Similarly, other researchers reported that higher levels of perceived techno-stress factors (overload, complexity, unreliability, insecurity, uncertainty, invasion) along with job role stressors (role- overload, role-conflict, and role ambiguity) create lower levels of intent to comply with ISPs and contribute to prospective non-compliance of ISP (Nasirpouri Shadbad and Biros 2021; Shadbad and Biros 2020).

Regardless of potential influencers of such behaviors, field studies nearly always employ multiple approaches to assess insiders' security-related behaviors as a DV which generally captures either actual behaviors or intention to perform security behaviors (Siponen and Vance 2013). Assessing actual behaviors are usually conducted in experimental settings and objective measures of compliance are collected (e.g., see study by Warkentin et al. 2016). However, measuring behavioral intent is also very common to determine the likelihood of individual compliance or noncompliance behaviors. Organizations would benefit from being able to assess risk efficiently and meaningfully in user behavior. One approach is employing self-reported behavior surveys (Curry et al. 2018, 2019; Marshall et al. 2022; Shadbad and Biros 2020) consisting of well-established indicators of intention that ask respondents to agree with assertions of behaving in accordance with the ISP (behavior survey) such as "I intend to comply with the requirements of the ISP of my organization in the future". This type of measurement leads to

obtaining a holistic understanding of individual ISP compliance (or non-compliance behaviors), whether, in general, they are willing to perform ISP requirements as prescribed.

Nonetheless, when it comes to a specific situation, behavior survey measures may not correctly reflect a behavioral intention to perform assigned ISS tasks, and individuals may violate certain ISPs. Due to the sensitivity of the topic and the challenges of observing employee ISP non-compliance, scenario-based experiments are pertinent to assess the likelihood of non-compliance (Siponen and Vance 2013; Wall and Warkentin 2019). Furthermore, researchers have an ethical responsibility not to ask respondents to self-incriminate. Consequently, the use of prospective non-compliance behavior scenarios (Shadbad and Biros 2021; Siponen et al. 2010; Vance et al. 2013) where someone similar to the respondent is described as violating an ISP end user agreement are a widely used proxy to assess prospective intent of non-compliance (prospective scenario) with ISP (Li et al. 2021; Siponen and Vance 2013) such as "I would have made the same decision as *[individual described as violating the ISP]* if I were in the same situation."

While the advantages and disadvantages of the behavior survey versus the prospective scenario approach are well discussed in the ISS literature (see, for example: Li et al. 2021; Moody et al. 2018; Siponen and Vance 2013) a significant gap is the lack of statistical evidence to show which is more accurate or compelling in indicating employee behavioral intention toward ISP compliance, and whether measures of non-compliance are the inverse of compliance. Practically, the concept of compliance and non-compliance are usually valued in a similar manner, where high levels of compliance imply low levels of non-compliance. As previously mentioned, ISS studies generally employ self-reported behavior surveys to assess ISP compliance and scenario-based surveys for non-compliance. Hence, one can interpret that the

reversed-scored items of behavior survey are representative of non-compliance behavior and it can be substituted as a scenario-based measure for assessing non-compliance behaviors. However, to the best of our knowledge, there is no empirical study to examine this issue and confirm the accuracy of such interpretation.

In the current study, we aim to fill this research gap through statistical analysis by comparing multiple theoretical models that explain compliance or non-compliance behaviors via self-reported behavior or prospect scenario-based surveys. Organizations may benefit from efficiently and meaningfully assessing user risk with psychometric surveys (Marshall et al. 2022), or other experimental approaches (e.g. phishing campaigns). However, each of these methods are expensive and may embarrass users. A better understanding of the indicative power of these assessment alternatives could help researchers as well as organizations more efficiently reduce vulnerabilities and fend off attacks. Consequently, our objective is to understand which measurement approach is most appropriate. Put another way, we assess the effectiveness of whether assessing ISP compliance is valid using either a behavior survey, prospect scenario, or both.

METHODOLOGY

To address our research question, we report on an effort to compare and contrast the results of two studies that employed different behavioral models (role-stress and techno-stress) and different dependent variables (prospective non-compliance and intent to comply). In Model 1, technostress was employed as a determinant of user behavior. Here, technostress was treated as a second-order construct reflected on six dimensions: techno-overload, techno-uncertainty, techno-invasion, technicality, techno-insecurity, and techno-unreliability. The items used for the

technostress construct were adopted from (Ragu-Nathan et al. 2008) and (Shadbad and Biros 2020). In Model 2, we used the role-stress construct consisting of role-overload, role-ambiguity, and role-conflict as the only independent variable measured using items from (Ayyagari et al. 2011; Ragu-Nathan et al. 2008). For both studies, the DV was measured in two ways. We used three items from (Bulgurcu et al. 2010) for the behavior survey to capture individuals' behavioral intention to comply with ISP. For prospect scenarios, participants were given six scenarios used in work by (Shadbad and Biros 2020). Their intention to not comply was measured using two items adapted from (D'Arcy et al. 2014) where the participants reported the likelihood of acting the same as the actor in the given scenario. They were also asked to rate the level of realism for the scenarios (to control its effect). The survey included all the constructs of the study for both models. We intentionally included both types of DV in a single survey to observe how one individual might respond to two different types of DVs at the same time. This way, we could better analyze the difference between two measures of DV. All items used a 7-point Likert scale from Strongly disagree to Strongly agree. The items used to measure the DV are included in Appendix A.

A marketing research company distributed an online survey among US employees with tech-related professions to collect data. Anonymous responses were collected from a sample of 400 participants. After cleaning data and removing incomplete responses, we used 354 observations for our analysis. Potentially impactful demographics including sex, age, education level, work experience, and industry were collected but proved to be of negligible effect.

In each model of the study, two types of DV were regressed on the independent variables, separately. Because the same respondents completed the surveys for both studies simultaneously, we can practically explore the overlap. Both models, individually, contributed to our

understanding of compliance (Nasirpouri Shadbad and Biros 2021) and non-compliance (Shadbad and Biros 2020), but together they offer a chance to explore (1) correlation between the two DVS in individuals, (2) the predictiveness of each of the models in predicting each of the DVs. In short, are the models measuring overlapping realities, and do the DV measures indicate a more general riskiness that includes both compliance and non-compliance elements?

RESULTS

Analysis of the data, focuses on two DV measures: the summed results from the behavior survey and standardized and summed values from the prospective scenario items. Recall that these measures are matched by respondent. Perceived scenario realism is also accounted for. In this section we report Pearson Correlation, present box and whisker charts that plot respondent answers to the two assessment approaches, and report on explained variance for the two causal models as it would be computed using the two inverse dependent variable values. As appropriate when using scenario results, respondents who reported perceiving the scenario as unrealistic (scenario realism < 5 out of 7) were omitted in computing and/or depicting correlation. This filtering eliminated 18% of the respondents but had little impact on the computations and depictions relationships.

The Pearson product-moment correlation coefficient between the summed survey and summed scenario responses was a moderate, negative relationship of -0.348 when all respondents were included (n=354) and -0.345 (n=291) after filtering out respondents who reported low perceived scenario realism with $p < .000001$ in both cases. This finding is highly significant .

To depict the relationship between the responses, we stratified them and compared their correlations. We observed a high degree of synchronicity in DV responses across the two measures. Figure 1 maps scenario responses to stratified levels of expressed intent to comply. Median, mean, and center quartile boxes move up as the stratified values increase, exhibiting the expected pattern of inverse correlation between measured propensity to violate and reported intent to comply. The four box and whisker plots represent 4 levels of expressed intent to comply. The first (on the left) represents 112 respondents who reported high levels of compliance intent by answering 6,7, and 7 on seven-point Likert scale questions. Corresponding prospective scenario scores thought to represent the likelihood of violation were relatively low with means (shown as an X) and median (shown as a line) well below those observed for the other strata. Within each strata the solid boxes represent the interquartile range (IQR). The IQR is the half of the responses in the second and third quartiles. Whisker lines extend either to the highest/lowest value or to a position 1.5 times the IQR above or below the first or third quartile. Outliers are shown as dots.

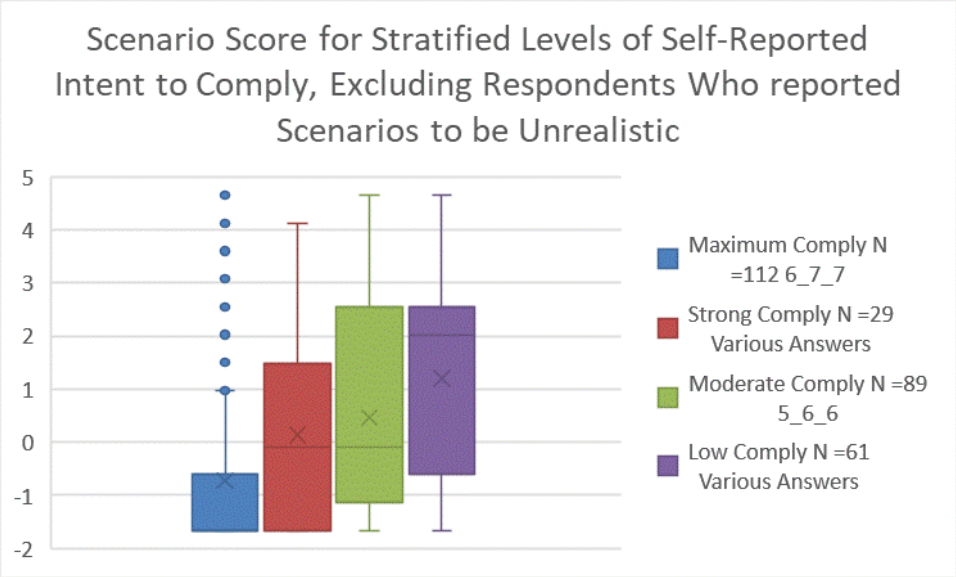

Figure 1. Scenario Scores by Intent-To-Comply Strata

Figure 2 maps the same results inversely. Intent to comply scores were mapped across four strata of scenario responses. This depiction would have been incrementally affected by inclusion of respondents who reported the scenarios were unrealistic. If all respondents had been included, the lower bounds of the boxes understandably stretched out the bottom of the graph to reflect more variation in responses.

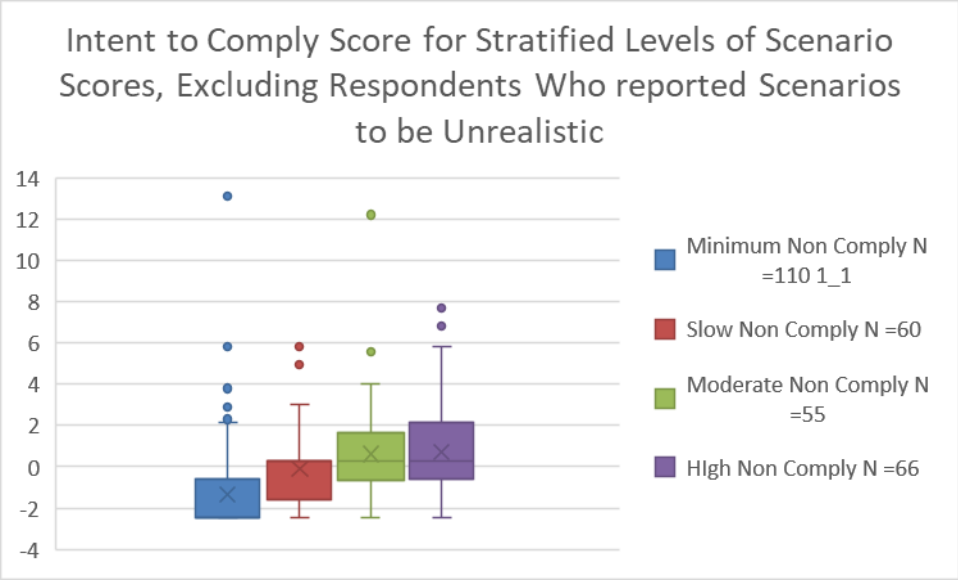

Figure 2. Intent-To-Comply Scores by Scenario Strata

In addition to observing the degree of synchronicity in DV responses across the two measures, we tested the main elements of the research models from two previous studies (i.e., technostress and role-stress), "swapping" the dependent variables. We tested both models with both prospective scenario and behavior survey dependent variable assessments. The results of the latent regressions models were displayed in Table 1. Both technostress and role-stress constructs showed significant effects on user behavior either through prospective scenario or behavior survey. However, the effect is stronger when the DV is intent to comply measured by behavior

survey. In addition, when the DV was substituted by the behavior survey, the observed shared variance (R^2) increased by 21.4% and 0.57% for technostress and role-stress models, respectively, which is a small effect size change (f^2) in both cases using Cohen's (1988) guidelines.

Table 1. Cross-matched Tested Models and Dependent Variable Measures

Model:	**Techno-Stress**	**Role-Stress**
Dependent Variable	Standardized path coefficient (R^2)	
Prospective Scenario (violate)	0.27*** (0.14)	0.27*** (0.14)
Behavior Survey (comply)	-0.41*** (0.17)	-0.47*** (0.22)
Effect Size†	0.03+	0.09+

*** p<.001

† Effect size (f^2) contrasting R^2 between scenario (violate) versus survey (comply) DVs.
Effect size: + = small, ++ = medium, +++ = large; according to Cohen's (1988) guidelines.

DISCUSSION

This article aims to provide evidence as to the magnitude of the overlap of prospective survey (violation focused) and behavior survey (compliance intention) measures of a respondent's compliance likelihood. In past studies, researchers have, with good reasons, chosen to use one or the other to measure these important proxies for compliance likelihood. Our unique data set, collected while two studies were performed in tandem, affords the opportunity for direct observation of the alignment of these two measures. Practitioners and researchers would expect that, while acknowledging the real possibility of variation from pattern, a respondent who is

more sympathetic to non-compliance scenarios would also be likely to report a lower intent to comply.

Figures 1 and 2 align with this intuitively satisfying, but previously unmeasured, supposition that propensity to violate and intent to comply are moderately and negatively correlated. Table 1 also supports this conclusion in that it showed that models based on techno-stress and role-stress theory would have been shown to be statistically significant using either of the two approaches to measuring user compliance propensity. The outliers depicted in Figure 1 show some respondents reported high intent to comply while still admitting they might not comply in some specific situations. This observation provides some evidence that measuring from both ends of the comply/non-comply spectrum can provide additional information.

Table 1 also showed that the behavioral survey intent to comply DV resulted in larger explained variance numbers given the same modeled drivers of behavior. The meaning of this incremental finding remains obscure. One could imagine that some research conducted using only scenario assessments might have failed to show significance when an effect would have been found had a different DV been used. On the other hand, the incremental increase in effect might be attributable to other experimental or statistical factors. These findings should give researchers additional information on which to base their qualitative assessments of future studies.

This study contributes to the ISS literature by reporting on systematically documented and significant levels of observed overlap between scenario-based violation-focused assessments and survey-based compliance focused measures. Of course, these observations are only a starting point. There is ambiguity associated with measuring compliance propensity by looking at one or the other side of the coin, and more research is needed to explore the degree to which

an intent to violate and an intent to comply overlap. It may well be that they are different phenomena that correlate due to shared drivers or experimental methodology, or it may be that, from a practical and theoretical standpoint, any difference between them is inconsequential.

Our analysis indicates that scenario and behavior survey measures were largely coherent and that both significantly validated theoretical models of compliance/non-compliance drivers. Thus, either seems workable in assessing user riskiness. In the studied data sets, assessing the compliance end of the compliance/non-compliance spectrum was better aligned with known drivers of risk-laden behavior. Though the effect size was small, using the compliance behavior surveys over the prospective scenario violation yielded stronger statistical results in both theoretical models. While this finding adds to a growing body of knowledge about how to identify risky users in organizations, it remains unclear whether the observed difference is due to the negative/positive valiance of the violation formulation, the prospective intention versus actual intention formulation of these measures, or both. Thus, more research is needed to determine whether these two formations actually assess the same thing.

ACKNOWLEDGEMENTS

This work was generously supported by University Information and Technology at Oregon State University.

REFERENCES

Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological Antecedents and Implications," *MIS Quarterly: Management Information Systems*. (https://doi.org/10.2307/41409963).

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *Management Information Systems Quarterly* (34:3), pp. 523–548.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, Routledge Academic.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-

Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly: Management Information Systems* (43:2), University of Minnesota, pp. 525–554. (https://doi.org/10.25300/MISQ/2019/15117).

Curry, M., Marshall, B., Crossler, R. . E., and Correia, J. 2019. "InfoSec Process Action Model (IPAM): Targeting Insider ' s Weak Password Behavior," *Journal of Information Systems*, pp. 1–51.

Curry, M., Marshall, B., Crossler, R. E., and Correia, J. 2018. "InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior," *Data Base for Advances in Information Systems* (49:S1), pp. 49–66. (https://doi.org/10.1145/3210530.3210535).

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285–318.

Li, H., Luo, X., Information, Y. C.-J. of the A. for, and 2021, undefined. 2021. "Understanding Information Security Policy Violation from a Situational Action Perspective," *Aisel.Aisnet.Org* (22:3), pp. 739–772. (https://doi.org/10.17705/1jais.00678).

Marshall, B., Curry, M., Crossler, R. E., and Correia, J. 2022. "Machine Learning and Survey-Based Predictors of InfoSec Non-Compliance," *ACM Transactions on Management Information Systems*. (https://doi.org/10.1145/3466689).

Moody, G., Siponen, M., Quarterly, S. P.-M., and 2018, U. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1).

Mou, J., Cohen, J. F., Bhattacherjee, A., Kim, J., Mou, J. ;, Cohen, J. F. ;, Bhattacherjee, A. ;, Cohen, J., and Thatcher, J. B. 2022. "A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach," *Journal of the Association for Information Systems* (23:1), Association for Information Systems, pp. 196–236. (https://doi.org/10.17705/1jais.00723).

Nasirpouri Shadbad, F., and Biros, D. 2021. "Understanding Employee Information Security Policy Compliance from Role Theory Perspective," *Journal of Computer Information Systems* (61:6), Taylor and Francis Ltd., pp. 571–580. (https://doi.org/10.1080/08874417.2020.1845584).

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., and Tu, Q. 2008. "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Validation," *Information Systems Research* (19:4), INFORMS Inst.for Operations Res.and the Management Sciences, pp. 417–433. (https://doi.org/10.1287/ISRE.1070.0165).

Shadbad, F. N., and Biros, D. 2020. "Technostress and Its Influence on Employee Information Security Policy Compliance," *Information Technnology & People* (35:1), Emerald Group Holdings Ltd., pp. 119–141. (https://doi.org/10.1108/ITP-09-2020-0610/FULL/XML).

Shadbad, F. N., and Biros, D. 2021. "Does Technostress Trigger Insider Threat? A Conceptual Model and Mitigation Solutions," *Information Technology in Organisations and Societies: Multidisciplinary Perspectives from AI to Technostress*, Emerald Publishing Limited, pp. 61–83. (https://doi.org/10.1108/978-1-83909-812-320211003/FULL/HTML).

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64–71.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly*, pp. 487–502.

(https://www.jstor.org/stable/25750688).

Siponen, M., and Vance, A. 2013. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:February 2012), pp. 1–17. (https://doi.org/10.1057/ejis.2012.59).

Trang, S., and Brendel, B. 2019. "A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research," *Information Systems Frontiers* (21:6), Springer, pp. 1265–1284. (https://doi.org/10.1007/S10796-019-09956-4/TABLES/8).

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), M.E. Sharpe Inc., pp. 263–290. (https://doi.org/10.2753/MIS0742-1222290410).

Verizon. 2022. "Data Breach Investigations Report." (https://www.magonlinelibrary.com/doi/pdf/10.12968/S1361-3723%2822%2970578-7).

Wall, J. D., and Warkentin, M. 2019. "Perceived Argument Quality's Effect on Threat and Coping Appraisals in Fear Appeals: An Experiment and Exploration of Realism Check Heuristics," *Information & Management* (56:8), North-Holland, p. 103157. (https://doi.org/10.1016/J.IM.2019.03.002).

Warkentin, M., Johnston, A. C., Shropshire, J., and Barnett, W. D. 2016. "Continuance of Protective Security Behavior: A Longitudinal Study," *Decision Support Systems* (92), North-Holland, pp. 25–35. (https://doi.org/10.1016/J.DSS.2016.09.013).

APPENDIX A -- DEPENDENT VARIABLE MEASURES

Intention to ISP compliance

CI1. I intend to comply with the requirements of the ISP of my organization in the future.

CI2. I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.

CI3. I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.

Scenarios

Password-sharing: Adam is an employee in your organization. One day while Adam is out of the office, one of his coworkers needs a file on Adams' computer. The coworker performs similar job functions to Adam's. The coworker calls Adams and asks for his account information. Although Adam knows your organization has a policy that password must not be shared, he shares his password with the coworker

Password write-down: John is an employee in your organization. The organization recently installed a computer system for managing employee personal information (e.g. employee emergency contacts, retirement benefits, salary information). Each employee has been given a username and password for the system. John is aware of the company policy stating 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, John wrote it down on a sticky note and attached it to the computer he usually uses.

Failure to logoff: Jim is an employee in your organization. As part of his job, Jim has been given authorized access to the company's payroll system. One day at work, Jim logs into the payroll system to gather information for a weekly report that he prepares for management. After some time, Jim needs a restroom break. He is aware of the company's policy that requires users to logoff their computers when not in use. However, Jim 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: Justin 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. Caleb 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, Caleb copies several company files to his personal, unencrypted USB drive so he can work on the report at home.

Data leakage: 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 providing the salary information is a violation of company policy, he looks it up and gives it to the friend.

Click on links: Nathan is an employee in your organization and receives many e-mails every day containing links that take him to fill out some forms. One day he receives an e-mail from an unknown sender. Even though it is against your organizations' policy to click on links without verifying the source of the e-mail, he clicks on the link assuming the e-mail is.

Intention to violate ISP

IV1. How likely is that you would have done the same as Adam in that situation? (very

unlikely/very likely)

IV2. I could see myself sharing the password as Adam did. (strongly disagree/strongly agree)

Scenario realism

SR. How realistic do you think the scenario is? (highly unrealistic, highly realistic)